

53-1000663-03  
26 March 2008



# EFC Manager Software

---

## User Manual

**BROCADE**

Copyright © 2006-2008 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, Fabric OS, File Lifecycle Manager, MyView, and StorageX are registered trademarks and the Brocade B-wing symbol, DCX, and SAN Health are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain "open source" software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit <http://www.brocade.com/support/oscd>.

## Brocade Communications Systems, Incorporated

Corporate Headquarters  
Brocade Communications Systems, Inc.  
1745 Technology Drive  
San Jose, CA 95110  
Tel: 1-408-333-8000  
Fax: 1-408-333-8101  
Email: [info@brocade.com](mailto:info@brocade.com)

Asia-Pacific Headquarters  
Brocade Communications Singapore Pte. Ltd.  
9 Raffles Place  
#59-02 Republic Plaza 1  
Singapore 048619  
Tel: +65-6538-4700  
Fax: +65-6538-0302  
Email: [apac-info@brocade.com](mailto:apac-info@brocade.com)

European and Latin American Headquarters  
Brocade Communications Switzerland Sàrl  
Centre Swissair  
Tour A - 2ème étage  
29, Route de l'Aéroport  
Case Postale 105  
CH-1215 Genève 15  
Switzerland  
Tel: +41 22 799 56 40  
Fax: +41 22 799 56 41  
Email: [emea-info@brocade.com](mailto:emea-info@brocade.com)

## Document History

Title	Publication number	Summary of changes	Date
EFC Manager Software User Manual	620-000170-000 Rev. A	Initial release of the manual to support release 8.0.	01 October 2003
EFC Manager Software User Manual	620-000170-010 Rev. A	Revised to support release 8.1.	01 January 2004
EFC Manager Software User Manual	620-000170-020 Rev. A	Revised to support release 8.5.	01 December 2004
EFC Manager Software User Manual	620-000170-030 Rev. A	Revised to support release 8.6.	01 February 2005
EFC Manager Software User Manual	620-000170-040 Rev. A	Revised to support release 8.7.	01 June 2005
EFC Manager Software User Manual	620-000170-050 Rev. A	Revised to support release 8.7.1.	01 September 2005
EFC Manager Software User Manual	620-000170-060 Rev. A	Revised to support release 8.8.	01 November 2005
EFC Manager Software User Manual	620-000170-070 Rev. A	Revised to support release 9.0.	01 September 2006
EFC Manager Software User Manual	620-000170-080 Rev. A	Revised to support release 9.1.	01 November 2006
EFC Manager Software User Manual	620-000170-090 Rev. A	Revised to change company name.	02 March 2007
EFC Manager Software User Manual	53-1000663-01 Rev. A.	Revised to support release 9.5.	31 July 2007
EFC Manager Software User Manual	53-1000663-02 Rev. A	Revised to support release 9.6.	19 October 2007
EFC Manager Software User Manual	53-1000663-03	Revised to support release 9.7.	26 March 2008



# Contents

---

## About this Document

How This Document is Organized .....	xv
Supported Hardware and Software .....	xvi
What's New in This Document .....	xvi
Document conventions .....	xvii
Text formatting .....	xvii
Notes, cautions, and warnings .....	xvii
Key terms .....	xviii
Additional information .....	xviii
Brocade resources .....	xviii
Other industry resources .....	xviii
Document feedback .....	xix

## Chapter 1

### Getting Started

In this Chapter .....	1
Overview .....	1
UDP and TCP Port Requirements .....	2
System Requirements .....	4
Server Requirements .....	4
Product Licensing Overview .....	8
License Keys .....	8
Feature Keys (Switch or Director Element Managers) .....	12
Installing the Application .....	13
Installing on Windows Systems .....	13
Installing on UNIX Systems .....	16
Headless Installation on UNIX Systems .....	18
Linux Installation Troubleshooting .....	20
Uninstalling the Application .....	21
Uninstalling from Windows Systems .....	21
Uninstalling from UNIX Systems .....	21
Headless Uninstall from UNIX Systems .....	22
Starting the Application .....	23
Starting EFCM on Windows Systems .....	23
Starting EFCM on UNIX Systems .....	24

Backing Up and Restoring Data .....	25
What is Backed Up? .....	25
Management Server Backup .....	26
Configuring Backup to a Writable CD .....	27
Configuring Backup to a Hard Drive .....	28
Configuring Backup to a Network Drive .....	29
Enabling Backup .....	30
Disabling Backup .....	30
Viewing the Backup Status .....	30
Changing the Backup Interval .....	31
Starting Immediate Backup .....	31
Reviewing Backup Events .....	32
Restoring Data .....	33
Restoring Data from the Brocade-Supplied Rack Mount Management Server .....	34
Restoring Data from CD .....	34
Restoring Data from the Hard Drive .....	35
Restoring Data from a Network Drive .....	36
Configuring Advanced Call Home .....	37
Showing a Call Home Center .....	39
Hiding a Call Home Center .....	39
Editing a Call Home Center .....	40
Enabling a Call Home Center .....	43
Testing the Call Home Center Connection .....	43
Disabling a Call Home Center .....	44
Viewing Call Home Status .....	45
Assigning a Device to the Call Home Center .....	46
Removing a Device From a Call Home Center .....	47
Removing All Devices and Filters From a Call Home Center ..	47
Defining an Event Filter .....	48
Assigning an Event Filter to a Call Home Center .....	48
Assigning an Event Filter to a Device .....	49
Overwriting an Assigned Event Filter .....	49
Removing an Event Filter from a Call Home Center .....	50
Removing an Event Filter from a Device .....	50
Removing an Event Filter from the Call Home Event Filters Table	50
Searching for an Assigned Event Filter .....	51
Miscellaneous .....	51
Multiple Network Interface Cards .....	51
Closing the Application .....	51
Using the Documentation .....	52
Searching the Online Help .....	52
Printing an Online Help Topic .....	52

## Chapter 2

### Software Overview

In this Chapter . . . . .	53
The Life Cycle of a SAN . . . . .	54
User Interface Description . . . . .	55
View Tab . . . . .	56
Product List . . . . .	56
Master Log . . . . .	58
Minimap . . . . .	59
Menu Bar . . . . .	60
Toolbar . . . . .	67
Toolbox . . . . .	68
Status Bar . . . . .	68

## Chapter 3

### Setting Up the Application

In this Chapter . . . . .	71
Server and Client Communication Requirements . . . . .	72
Configuring a Server . . . . .	73
Logging In to a Server . . . . .	73
Changing Your Password . . . . .	74
Logging Out of a Server . . . . .	74
Adding a Server . . . . .	75
Viewing Server Properties . . . . .	76
Configuring HBAs and Servers . . . . .	77
Removing a Server . . . . .	78
Configuring the Client . . . . .	79
Configuration Options . . . . .	79
Configuring Backup Settings . . . . .	79
Configuring End Node Display . . . . .	80
Configuring Flyover Settings . . . . .	80
Configuring FTP Server Settings . . . . .	81
Configuring Nickname Settings . . . . .	82
Editing Duplicate Nicknames . . . . .	82
Configuring Reset Display Settings . . . . .	83
Configuring Software Settings . . . . .	84
Managing Users . . . . .	89
Viewing the List of Users . . . . .	89
Adding a User Account . . . . .	90
Changing a User Account . . . . .	91
Removing a User Account . . . . .	91
Filtering Event Notifications for a User . . . . .	92
Setting Up Advanced Event Filtering . . . . .	93

Managing User Groups .....	94
Creating a User Group .....	94
Editing a User Group .....	96
Removing a User Group .....	97
Assigning Users to Groups .....	98
Removing a User from a Group .....	99
Finding a User's Groups .....	99
Configuring Remote Access .....	100
Viewing Active User Sessions .....	101
Partitioned Switch Support .....	102
Viewing the Logical Configuration of Devices .....	102
Customizing the Main Window .....	103
Zooming In and Out of the Physical Map .....	103
Showing Levels of Detail on the Physical Map .....	104
Turning Flyovers On or Off .....	104
Viewing Flyovers .....	104
Customizing Device Properties .....	105
Adding a Property Field .....	105
Editing a Property Field .....	105
Deleting a Property Field .....	106
Hiding a Property Field .....	106
Hiding All Empty Property Fields .....	107
Showing a Property Field .....	107
Showing All Property Fields .....	107
Showing Only Property Fields with Data .....	108
Export and Import .....	109
Exporting Data to Disk or E-mail .....	109
Selecting an E-Mail Address for Export .....	112
Defining Filters for Export .....	112
Exporting Data to a Database .....	113
Importing Data .....	116
Accessing Third-Party Tools .....	123
Adding a Tool .....	123
Adding an Option to the Tools Menu .....	124
Changing an Option on the Tools Menu .....	125
Removing an Option from the Tools Menu .....	125
Adding an Option to a Device's Shortcut Menu .....	126
Changing an Option on a Device's Shortcut Menu .....	127
Removing an Option from a Device's Shortcut Menu .....	127
Launching a Telnet Session .....	127
Launching an Element Manager .....	128
Launching Web Tools .....	128
Launching FCR Configuration .....	129
Starting Third-Party Tools from the Application .....	129
Accessing Eclipse Management Applications .....	130

## Chapter 4

## Discovering a SAN

In this Chapter . . . . .	131
How Discovery Works . . . . .	132
Out-of-Band Discovery . . . . .	132
In-Band Discovery . . . . .	132
DataFabric Manager Interaction Requirements . . . . .	133
Gathering DataFabric Manager Device Discovery Data . . . . .	133
SNMP Trap Listener Conflict . . . . .	133
Manager of Manager Discovery . . . . .	134
Discovering Data From Another EFCM Server . . . . .	135
License Discovery . . . . .	137
Mi10K Director Discovery . . . . .	138
Access Gateway Discovery . . . . .	138
N_Port ID Virtualization Discovery . . . . .	139
Setting Up Discovery . . . . .	139
Setting the Polling Delay . . . . .	141
Configuring Address Properties . . . . .	142
Adding an IP Address . . . . .	142
Editing an IP Address . . . . .	144
Enabling Extended Discovery . . . . .	145
Disabling Extended Discovery . . . . .	146
Removing an IP Address . . . . .	147
Configuring an SNMP Community String . . . . .	147
Reverting to a Default SNMP Community String . . . . .	149
Configuring the Product Type and Access . . . . .	<b>149</b>
Turning Discovery On and Off . . . . .	151
Determining the Discovery State . . . . .	151
Troubleshooting Discovery . . . . .	152
Configuring Storage Port Mapping . . . . .	155
Adding Storage Ports to a Storage Array . . . . .	156
Removing Storage Port and Storage Array Associations . . . . .	156
Reassigning Mapped Storage Ports . . . . .	157
Creating a Storage Array . . . . .	157
Editing Storage Array Properties . . . . .	158
Deleting a Storage Array . . . . .	159
Viewing Storage Port Properties . . . . .	159
Viewing Storage Array Properties . . . . .	160

## Chapter 5

## Configuring SAN Products and Fabrics

In this Chapter .....	161
Managing Products .....	162
Determining Whether a Product is Being Managed .....	162
Opening a Product's Element Manager .....	162
Searching for Products in a SAN .....	163
Changing Product Properties .....	163
Determining a Product's Operational Status .....	164
Showing Routes Between Two End-Products .....	165
Hiding Routes Between Two End-Products .....	166
Viewing Properties of Routes Between Two End-Products ..	166
Changing a Fabric's Properties .....	166
Configuring Nicknames .....	167
Viewing Nicknames .....	167
Searching by Nickname .....	168
Searching by WWN .....	169
Assigning a Nickname to an Existing Device .....	170
Adding a Nickname to a New Device .....	170
Importing Nicknames .....	171
Importing FC Aliases into Nicknames .....	172
Exporting Nicknames .....	172
Removing a Nickname .....	173
Configuring Enterprise Fabric Mode .....	174
About Enterprise Fabric Mode .....	174
Setting Enterprise Fabric Mode .....	175
Configuring Fabric Binding .....	176
Fabric Binding and Element Manager Switch Binding for Blade Switches .....	177
Enabling Fabric Binding .....	178
Disabling Fabric Binding .....	179
Adding Switches to the Fabric Binding Membership List ...	179
Adding Detached Devices to the Fabric Binding Membership List	180
Removing Switches from Fabric Binding Membership .....	181
Port Fencing .....	182
Thresholds .....	183
Adding Thresholds .....	184
Assigning Thresholds .....	187
Turning Off Port Fencing Inheritance .....	188
Editing Thresholds .....	189
Finding Assigned Thresholds .....	191
Viewing Thresholds .....	192
Removing Thresholds .....	192

Persisting and Unpersisting Fabrics and Switch Groups .....	194
Persisting a Fabric or Switch Group .....	194
Unpersisting a Fabric or Switch Group .....	194
Unpersisting a Single Product .....	194
Graphic Indicators Related to Persisted Fabrics .....	195
Merging Persisted Fabrics .....	196
Splitting Persisted Fabrics .....	196
Layout Changes in Persisted Fabrics .....	196
Finding Devices in a Persisted Fabric .....	197
Configuring Trap Forwarding .....	197
Configuring Trap Forwarding .....	197
Adding Trap Recipients .....	198
Removing Trap Recipients .....	198
Configuring Frame Sniffer .....	199
Frame Sniffer Requirements .....	199
Viewing Frame Sniffer Tests .....	200
Adding a New Frame Sniffer Test .....	201
Running a Frame Sniffer Test .....	202
Stopping a Frame Sniffer Session .....	203
Editing a Frame Sniffer Test .....	204
Deleting a Frame Sniffer Test .....	205
Deleting a Frame Sniffer Session .....	205
Refreshing the Frame Sniffer .....	206
Configuring the SNMP Agent .....	207
Setting Up the SNMP Agent .....	207
Turning On the SNMP Agent .....	208
Turning Off the SNMP Agent .....	208
Adding Trap Recipients .....	209
Editing Trap Recipients .....	210
Changing the UDP Port .....	211
Removing Trap Recipients .....	211
Adding Community Strings .....	212
Editing Community Strings .....	213
Removing Community Strings .....	213
Changing the TCP/IP Port for SNMP Trap Events .....	214

## Chapter 6

### Monitoring SAN Products

In this Chapter .....	215
Event Monitoring .....	216
Viewing Logs .....	216
Clearing Logs .....	217
Exporting Log Data .....	217
Deleting Group Logs .....	218
Viewing the Fabric Log .....	218
Filtering Events in the Master Log .....	218
Copying Log Entries .....	219
Using Event Notification Features .....	220
Configuring E-mail Notification .....	220
Enabling Ethernet Events .....	222

	Creating Reports . . . . .	223
	Generating Reports . . . . .	224
	Viewing Reports . . . . .	225
	Printing Reports . . . . .	226
	Printing a Connectivity Map Report . . . . .	226
	Deleting Reports . . . . .	227
	Generating Router Reports . . . . .	227
	Generating Zone Library Reports . . . . .	228
<b>Appendix A</b>	<b>Troubleshooting</b>	
	In this Appendix. . . . .	229
	Problems with Addresses . . . . .	229
	Problems with Discovery. . . . .	230
	Problems with Fabric Binding. . . . .	233
	Problems with LUNs . . . . .	233
	Problems with Products . . . . .	234
	Miscellaneous Problems . . . . .	234
<b>Appendix B</b>	<b>Editing Configuration Properties Files</b>	
	In this Appendix. . . . .	237
	Specifying a Host IP Address in Multi-NIC Networks . . . . .	238
	Editing Master Log Settings . . . . .	238
	Configuring the ECCAPI Port Number . . . . .	239
	Configuring the CLI Proxy Listening Port Number. . . . .	239
<b>Appendix C</b>	<b>Reference</b>	
	In this Appendix. . . . .	241
	Compatibility with Other Applications . . . . .	242
	Changing the TCP/IP Port for SNMP Trap Events. . . . .	242
	Icon Legend . . . . .	243
	Keyboard Shortcuts . . . . .	247
<b>Appendix D</b>	<b>Configuring EFCM Through a Firewall</b>	
	In this Appendix. . . . .	249
	Polling Client Function . . . . .	250
	Configuring for Faster Logins . . . . .	250
	Configuring TCP Port Numbers to Allow Firewall Access . . . . .	252
	EFCM with RMI at TCP Port Level . . . . .	252
	Forcing Port in RMI Registry . . . . .	253
	Forcing Server and Client Export Port Number . . . . .	253

## **Appendix E**

### **MySQL and DB2 Database Fields**

In this Appendix. . . . .	255
MySQL and DB2 Database Fields . . . . .	256
ADAPTER Table. . . . .	257
CONNECTION Table . . . . .	257
DEVICE Table . . . . .	258
FABRIC Table . . . . .	258
HISTORICALPERFORMANCE Table . . . . .	259
HOST Table. . . . .	259
HOSTCONNECTION Table . . . . .	260
HOSTHBAS Table . . . . .	260
HOSTLUNS Table . . . . .	261
IFCPLINK Table. . . . .	261
LUN Table . . . . .	262
LUNBINDING Table . . . . .	262
LUNMASKING Table. . . . .	263
MSAN Table . . . . .	263
NETAPPFILER Table. . . . .	264
PORT Table. . . . .	264
REALTIMEPERFORMANCE Table. . . . .	265
ROUTERFABRIC Table . . . . .	265
SANROUTERSYSTEM Table . . . . .	266
STORAGEDEVICES Table . . . . .	266
ZONE Table. . . . .	267
ZONELIBRARY Table . . . . .	268
ZONEMEMBER Table . . . . .	268
ZONEMEMBERDOMAINPORT Table . . . . .	269
ZONEMEMBERFABRICADDRESS Table . . . . .	269
ZONEMEMBERWWN Table . . . . .	269
ZONESET Table . . . . .	270
ZONESETZONES Table. . . . .	270

## **Appendix F**

### **User Privileges**

In this Appendix. . . . .	271
About User Privileges . . . . .	272
About User Groups and Access Levels . . . . .	285

## **Appendix G**

### **Advanced Call Home Event Tables**

In this Appendix. . . . .	287
---------------------------	-----

## **Appendix H**

### **B Model Considerations**

In this Appendix. . . . .	293
B Model Supported Traps. . . . .	293

## **Index**



# About this Document

---

This publication provides instructions on using the EFC Manager (EFCM) application.

---

**NOTE**

To improve readability, this document refers to the release number of the application as “9.7” instead of the official release number “09.07.00”.

---

- [How This Document is Organized](#) ..... xv
- [Supported Hardware and Software](#) ..... xvi
- [What’s New in This Document](#) ..... xvi
- [Document conventions](#) ..... xvii
- [Additional information](#) ..... xviii
- [Document feedback](#) ..... xix

## How This Document is Organized

This publication is organized as follows:

[Chapter 1, \*Getting Started\*](#), provides system requirements and basic configuration instructions.

[Chapter 2, \*Software Overview\*](#), provides a high-level overview of the user interface.

[Chapter 3, \*Setting Up the Application\*](#), describes how to set up and customize the application to manage users and user groups, set up servers and clients, customize the main window, customize device properties, and import or export files.

[Chapter 4, \*Discovering a SAN\*](#), describes how to discover SANs and configure storage port mapping using the application.

[Chapter 5, \*Configuring SAN Products and Fabrics\*](#), describes how to configure the SAN devices. Topics include managing devices, configuring nicknames, enterprise fabric mode, fabric binding, port fencing, trap forwarding, frame sniffer, and SNMP agent, as well as working with HBAs and servers.

[Chapter 6, \*Monitoring SAN Products\*](#), describes how to monitor the SAN’s events and how to create reports that show information about the SAN.

[Appendix A, \*Troubleshooting\*](#), provides a list of common problems with and recommended solutions.

[Appendix B, \*Editing Configuration Properties Files\*](#), provides instructions for editing configuration properties files to perform various tasks.

[Appendix C, \*Reference\*](#), provides supplemental information including compatibility information, an icon legend, and keyboard shortcuts.

[Appendix D, \*Configuring EFCM Through a Firewall\*](#), provides information on configuring through a firewall.

[Appendix E, MySQL and DB2 Database Fields](#), provides reference information related to database exporting.

[Appendix F, User Privileges](#), provides supplemental information about user privileges and access levels.

[Appendix G, Advanced Call Home Event Tables](#), provides supplemental information about the specific events that display when using Advanced Call Home.

[Appendix H, B Model Considerations](#), provides supplemental information about the specific considerations you need to know when using B model devices.

The [Glossary](#) defines terms, abbreviations, and acronyms used in this manual.

An *Index* is also provided.

## Supported Hardware and Software

This document supports the following platforms:

- All B model switches and directors
- All M model switches, directors, and SAN routers
- FOS 5.3 or later
- M-EOS and M-EOSn 9.7

In those instances in which procedures or parts of procedures documented here apply to some switches but not to others, this guide identifies exactly which switches are supported and which are not.

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc., documenting all possible configurations and scenarios is beyond the scope of this document.

## What's New in This Document

The following changes have been made since this document was last released:

- Information that was added:
  - IPv6 address support.
- Information that was changed:
  - Technical Edits.
- Information that was removed:
  - None.

For further information, refer to the release notes.

# Document conventions

This section describes text formatting conventions and important notices formats.

## Text formatting

The narrative-text formatting conventions that are used in this document are as follows:

<b>bold text</b>	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
<i>italic text</i>	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
<code>code text</code>	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, switchShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

## Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

---

### NOTE

A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

---



---

### ATTENTION

An Attention statement indicates potential damage to hardware or data.

---




---

### CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you.

---




---

### DANGER

*A Danger statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.*

---

## Key terms

For definitions specific to Brocade and Fibre Channel, see the **Brocade Glossary**.

For definitions specific to EFCM, see the “**Glossary**” on page 295.

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

<http://www.snia.org/education/dictionary>

## Additional information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

### Brocade resources

To get up-to-the-minute information, join Brocade Connect. It's free! Go to <http://www.brocade.com> and click **Brocade Connect** to register at no cost for a user ID and password.

For practical discussions about SAN design, implementation, and maintenance, you can obtain **Building SANs with Brocade Fabric Switches** through:

<http://www.amazon.com>

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

<http://www.brocade.com>

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

### Other industry resources

- White papers, online demos, and data sheets are available through the Brocade Web site at <http://www.brocade.com/products/software.jhtml>.
- Best practice guides, white papers, data sheets, and other documentation is available through the Brocade Partner Web site.

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, and other applications:

<http://www.t11.org>

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

<http://www.fibrechannel.org>

## Document feedback

Because quality is our first concern at Brocade, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to:

`documentation@brocade.com`

Provide the title and version number of the document and as much detail as possible about your comment, including the topic heading and page number and your suggestions for improvement.



# Getting Started

---

## In this Chapter

This chapter provides information to help you begin using the EFCM application.

• Overview . . . . .	1
• System Requirements . . . . .	4
• Product Licensing Overview . . . . .	8
• Installing the Application . . . . .	13
• Uninstalling the Application . . . . .	21
• Starting the Application . . . . .	23
• Backing Up and Restoring Data . . . . .	25
• Configuring Advanced Call Home . . . . .	37
• Closing the Application . . . . .	51
• Searching the Online Help . . . . .	52

## Overview

EFCM Release 9.7 is available for installation on a management server supplied by Brocade or IBM or your own management server. EFCM for UNIX systems includes all of the features of EFCM except for the Advanced Call Home and Backup features.

---

### NOTE

Advanced Call Home is only available on Windows and Solaris systems. Backup is only available on Windows systems.

---

The SAN Management application has the following client and server system requirements.

#### Enterprise Edition License

- A maximum of 25 Clients are allowed per Server.
- The Server supports unlimited discovered ports.

#### Standard Edition License

- A maximum of 2 Clients are allowed per Server.
- The Server supports up to 140 discovered ports.

## UDP and TCP Port Requirements

The following tables detail the port numbers used by EFCM, and note where the ports are used for client- server connectivity as well as for product management of the suite of Brocade products.

### NOTE

If the default ports defined are not available, the associated feature becomes unavailable.

**TABLE 1** EFCM Server Ports Used by Other Applications (Including EFCM client)

Port	UDP/ TCP	Feature	Client/Server	Product Management	Editable
51513	TCP	ECCAPI			YES
51512	TCP	CLI Proxy from client to managed product			YES
51511	TCP	RMI registry	YES		YES
51510	TCP	RMI calls from <b>EFCM</b> client	YES		YES
4033	UDP	Peer manager			
1024	UDP	SNMP traps from Mi10K director		YES	
162	UDP	SNMP traps (can be forwarded or create events)		YES	YES
80	TCP	Client download			

You can edit the following default port numbers. However, some changes require coordinated changes on the managed products.

To edit the ECCAPI port number (51513), refer to [“Configuring the ECCAPI Port Number”](#) on page 239.

To edit the CLI Proxy from client to managed product port number (51512), refer to [“Configuring the CLI Proxy Listening Port Number”](#) on page 239.

To edit the RMI registry port number (51511), refer to [“Configuring Server Connection Settings”](#) on page 88.

To edit the RMI calls from the EFCM Client port number (51510), refer to [“Configuring Server Connection Settings”](#) on page 88.

To edit the SNMP traps port number (162), refer to [“Configuring SNMP Trap Listening Settings”](#) on page 88.

**TABLE 2** Other Application Ports Used by the EFCM Server

Port	UDP/ TCP	Feature	Client/Server	Product Management	Editable
55555	TCP	RMI calls to <b>EFCM</b> client	YES		YES
8080	TCP	XML-RPC (zoning, bb-credit, statistics)		YES	
4430	TCP	XML-RPC (zoning, bb-credit, statistics) (Secure)		YES	
2049	TCP	<b>EFCM</b> server to device (3016, 3032, 3216, 3232, 4400, 4500, 4700, 6064, and 6140) (SSL)		YES	
2048	TCP	<b>EFCM</b> server to device (3016, 3032, 3216, 3232, 4400, 4500, 4700, 6064, and 6140)		YES	
575	TCP	Call home via call home service			
161	UDP	SNMP query		YES	
25	TCP	E-mail notifications via SMTP server			YES

You can edit the following default port numbers. However, some changes require coordinated changes on the managed products.

To edit the RMI calls to the EFCM Client port number (55555), refer to [“Configuring Client Export Port Settings”](#) on page 84.

To edit E-mail notification via SMTP server port number (25), refer to [“Configuring E-mail Notification”](#) on page 220.

# System Requirements

## NOTE

When managing large fabrics, we recommend that you use a platform meeting at least the recommended requirements for both server and client.

For the latest device-compatibility information (including model number and firmware levels) please go to the <http://www.brocade.com/support/resources> website and follow the instructions to access the Compatibility Matrix.

## Server Requirements

## NOTE

When managing large fabrics, we recommend that you use a platform meeting at least the recommended requirements for both server and client.

You have the choice of running the SAN Management application on a management server supplied by Brocade or IBM or providing your own management server. When using a management server supplied by Brocade or IBM, the recommended configuration is already set. However, when using your own management server, use the following recommendations for your platform.

**TABLE 3** 1 U Server Requirements

	Minimum	Recommended
<b>Processor</b>	2.0 GHz Intel Pentium 4	3.0 GHz Intel Pentium 4
<b>Hardware</b>	CD-ROM	CD-ROM
<b>Operating System</b>	Windows 2000 Professional with service pack 4 <b>NOTE:</b> IPv6 addresses are not supported in Windows 2000.	Windows 2003 Server Standard Edition with service pack 1
	Windows 2003 Server Standard Edition with service pack 1	
<b>Memory</b>	1 GB	2 GB
<b>Graphics Card</b>	8MB VGA-256	32 MB VGA-256
<b>Hard Drive</b>	40 GB	40 GB ATA-100 IDE (7200 rpm)
<b>Modem</b>	56K, v.92 data/fax modem, PCI	56K, v.92 data/fax modem, PCI
<b>Ethernet NIC</b>	10/100 Mbps Ethernet LAN card	10/100 Mbps Ethernet LAN card

**TABLE 4** Windows Server Requirements

<b>Processor</b>	2.0 GHz Intel Pentium 4
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Windows 2000 Professional with service pack 4 <b>NOTE:</b> IPv6 addresses are not supported in Windows 2000. Windows 2000 Server with service pack 4 Windows 2000 Advanced Server with service pack 4 Windows Server 2003 Enterprise Edition with service pack 1 Windows XP with service pack 2
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB VGA-256
<b>Resolution</b>	256 colors

**TABLE 5** Solaris Server Requirements

<b>Processor</b>	Solaris UltraSparc III and up
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Solaris 9 or 10
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB 8-bit color
<b>Resolution</b>	256 colors

**NOTE**

Approximately 1.3 GB of space is necessary on the /tmp directory of Solaris systems to install the application.

**NOTE**

EFCM for Solaris, includes all of the features of EFCM except the Backup feature.

# 1 System Requirements

**TABLE 6** Linux Server Requirements

<b>Processor</b>	2.0 GHz Intel Pentium 4
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Red Hat Enterprise Linux ES 3.0 Red Hat Enterprise Linux ES 4.0 Redhat 9.0 kernel v. 2.4.20-8 SuSE Linux 9.2 SuSE Linux 9.3
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB 8-bit color
<b>Resolution</b>	256 colors

---

**NOTE**

When managing large fabrics, we recommend that you use a platform meeting at least the recommended requirements for both server and client.

---

The Client system running the SAN Management application must meet the following requirements.

**TABLE 7** Windows Client Requirements

<b>Processor</b>	2.0 GHz Intel Pentium 4
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Windows 2000 Professional with service pack 4 <b>NOTE:</b> IPv6 addresses are not supported in Windows 2000. Windows 2000 Server with service pack 4 Windows 2000 Advanced Server with service pack 4 Windows Server 2003 Enterprise Edition with service pack 1 Windows XP with service pack 2
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB VGA-256
<b>Resolution</b>	256 colors

**TABLE 8** Solaris Client Requirements

<b>Processor</b>	Solaris UltraSparc III and up
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Solaris 9 or 10
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB 8-bit color
<b>Resolution</b>	256 colors

**TABLE 9** Linux Client Requirements

<b>Processor</b>	2.0 GHz Intel Pentium 4
<b>Hardware</b>	CD-ROM
<b>Operating System</b>	Red Hat Enterprise Linux ES 3.0 Red Hat Enterprise Linux ES 4.0 Redhat 9.0 kernel v. 2.4.20-8 SuSE Linux 9.2 SuSE Linux 9.3
<b>Memory</b>	1 GB
<b>Disk Space</b>	2 GB
<b>Video Requirements</b>	8MB 8-bit color
<b>Resolution</b>	256 colors

## Product Licensing Overview

License keys are unique strings of alphanumeric characters that verify ownership of the SAN Management application software as well as determine any additional features (such as, Event Management) that you receive as part of the license.

Feature keys are unique strings of alphanumeric characters that verify ownership of Switches and Directors as well as any additional software features within the Switches or Directors that you purchase.

### License Keys

License keys allow you to access the features that you purchase with the SAN Management application software package. Depending on the software package you purchase, you may have any of the features in the following table.

**TABLE 10** EFCM Software Features

Features	Standard Edition	Enterprise Edition
Advanced SAN Routing	X <sup>o</sup>	X <sup>o</sup>
<b>Advanced Module</b> Event Management Group Configuration Performance Security		X <sup>o</sup>
<b>Backup</b>	X	X
<b>Advanced Call Home</b> (Windows and Solaris only)	X	X
<b>Planning</b>		X
<b>Basic SAN Routing</b>	X	X
<b>View Management</b>	X	X
<b>Virtual Fabrics</b>	X	X
<b>Zoning</b>	X	X
<sup>o</sup> Optional module.		

Note the following items regarding the SAN Management software application for this release:

- In the **License** dialog box, the **Adv Module Licensed Ports** field indicates the number of ports for which you have licenses for the optional software modules.
- The number of ports in the licensed optional software modules must be equal to or greater than the number of currently discovered ports.
- All of the software modules that are port-based must have the same number of ports activated. For example, if you have 128 ports for Performance and want to add the Event Management module, you must purchase 128 ports for Event Management.
- The serial number cannot be changed without reinstalling the software.

Depending on whether you are installing for the first time, adding additional features, adding ports, or upgrading to a new version, you need to complete the following steps.

- Obtain the license key
- Enter the software serial number
- Enter the license key

Table 1-12 outlines which steps you must perform to complete the installation or upgrade process.

**TABLE 11** License Key Requirements

	Obtain License Key	Enter Serial Number	Enter License Key
<b>Install the software application for the first time</b>	X <sup>1</sup>	X	X
<b>Purchase Additional Software Modules</b>	X		X
<b>Purchase Ports</b>	X		X
<b>Upgrade EFCM</b>	X	X	X

1. Depending on your vendor, you may or may not receive the license key directly and consequently, skip this step.

## Obtaining a License Key

To activate the application, you must request a license key. If you just purchased the application, use these instructions to obtain your license key.

1. Go to the URL listed on the transaction code certificate.
2. Enter your username and password and click **Login**.  
**NOTE:** If you do not have a username and password, click the **Please Register Here** link.
3. In the **Serial Number** field, type the serial number.  
The serial number on the back of the software CD case.
4. In the **Transaction Code** fields, type the transaction codes shipped with the software and click **Next**.
5. Confirm the features to be enabled and click **Next**.  
The license key and all enabled features display.
6. Print or e-mail the license key and enabled features information to retain a copy for your records.

Enter this key during the installation process. For step-by-step instructions for installation, refer to [“Installing the Application”](#) on page 13.

**TIP:** To e-mail a copy of the license key and enabled feature information, type an e-mail address in the E-mail Key To field and click Send.

**TIP:** To print the certificate and instructions, use the Certificate and Instructions links.

## Requesting a License Key

1. Go to the Brocade Product Feature Enabling System for Hardware and Software web page at <http://mcdata.getkeys.com/>.

2. Enter your username and password and click **Login**.

**NOTE:** If you do not have a username and password, click the **Please Register Here** link.

3. In the **Serial Number** field, type the serial number and click **Next**.

You can find the serial number on the back of the software CD case.

The license key and all enabled features are displayed.

4. Print or e-mail the license key and enabled features information to retain a copy for your records.

You need to enter this key during the installation process. For step-by-step instructions for installation, refer to “[Installing the Application](#)” on page 13.

## Ordering Additional Features

To order new features or increase managed port capabilities, contact your sales representative or the Solution Center at (877) 948-4448 or (303) 327-2121.

## Entering the License Key

A license key is required to run the application. The key specifies the maximum number of switch ports you can monitor, the number of clients you can run, the expiration date of a trial license, as well as any licensed optional modules. Before you enter the license key you must install the application, for step-by-step instructions on installation, refer to “[Installing the Application](#)” on page 13.

1. Select **Help > License**.

The **License** dialog box displays ([Figure 1](#)).

Serial #

License Key

Update

Discovered Ports 165

Adv Module 4096

Licensed Ports

☐ Aggregate advanced module licensed port counts from all managed EFCM servers

Advanced Module

Details

[Performance Management](#) ✓

[Event Management](#)

[Group Configuration](#)

[Security Center](#)

Performance Management

Performance Monitoring measures the current performance statistics, historic metrics and future trends of every switch port on your SAN. Performance Monitoring identifies links and ports within the storage network that are over- and under-utilized. Network performance management means more ports available to storage arrays. Leverage this information to make

Contact sales at [www.brocade.com](http://www.brocade.com), 1-800-545-5773

OK Cancel Help

**FIGURE 1** License Dialog Box

2. If you are upgrading from a trial license, enter the serial number.

3. In the **License Key** field, enter the license key.

The **License Key** field is not case-sensitive.

The **License** dialog box displays the license information for the Server to which the Client is currently connected.

4. Click **Update** and confirm that the information is accurate.

The dialog box decodes the key you entered and displays the new license information without setting a new license on the Server.

The **Adv Module Licensed Ports** field port count is calculated using the following criteria:

- Displays the number of licensed ports when the license key has at least one advanced module licensed. Only directly discovered switches are counted for licensing. This includes the following:
  - Direct discovery: All devices whose IP address is specified in the Discovery Setup dialog box.
  - Subnet discovery: All devices discovered as a result of the subnet broadcast.
  - Manager of Managers discovery: All devices discovered as part of MoM discovery are counted.
- Displays "N/A" if the license key has no advanced modules.
- Displays with the EFCM 9.5 behavior when the discovered port count meets the following condition:  
 $Discovered\ port\ count > Licensed\ port\ count + grace\ port\ count$

If your port count exceeds your license, the following messages display in the topology;

- Displays a water mark with the text, *"License Exceeded. See Help > License for details"* if the discovered port count exceeds your license, but is within the grace period range.
- Displays *"The current number of managed ports exceeds your license of x ports. You have a buffer range of up to y ports before functionality is limited. Please contact your storage vendor to purchase additional port licenses or reduce the number of ports being discovered through the Discovery Setup dialog box."* if the discovered port count exceeds your license and the grace period.

5. Click **OK** to enable the software.

The information will be set on the Server only after you click **OK**.

The client automatically logs out and the EFCM 9.7 Log In dialog box displays. Log in using the instructions in ["Logging In to a Server"](#) on page 73.

## Retrieving Lost Keys

If you have lost your license key, complete these steps.

1. Go to the URL listed on the transaction code certificate.
2. Enter your username and password and click **Login**.
3. Click the **Unit Information** menu.
4. Enter your product's serial number or key and click **Next**.

The product license information displays.

## Feature Keys (Switch or Director Element Managers)

Feature keys allow you to access the software features that you purchase within the Switch or Director. The feature key, which is encoded with a Switch or Director's serial number, can only be configured on the Switch or Director to which it is assigned. Following are some important notes about the Element Manager feature key for this release:

- Enabling the Reset Configuration option through the Element Manager Maintenance menu clears all features that were enabled through the Configure Feature Key dialog box. When you attempt to re-install features using a feature key assigned for version M-EOS 5, a warning displays that the feature key is not installed. You must contact customer support to re-assign a feature key.
- Directors with M-EOS 6.0 or later installed have feature keys for all previously purchased software features activated automatically.
- Switches with M-EOS 6.0 or later installed need a feature key to enable the Element Manager and any other additional keyed software features within the switch.
- When you purchase additional software features for a Director or Switch, you receive a new feature key that includes existing features purchased previously. To activate the new features, refer to the **Configure Feature Key** dialog box in the Switch or Director Element Manager User Manual.

# Installing the Application

Follow these instructions to install the application on your system. To migrate data from a previous version or for more information about upgrade considerations, refer to the EFCM Upgrade Instructions.

The Upgrade Instructions are available on the documentation CD or, if you run the documentation installer from the documentation CD, you can access this document in <Install\_Home>\docs\.

**TIP:** On Windows systems, if you run the documentation installer, you can also access documentation through the Windows Start menu. Browse to the application's submenu and select Documentation.

---

## NOTE

SANavigator Software and EFCM Software cannot be run on the same machine, even if one of the products is running as a service.

---

## Installing on Windows Systems

Follow these instructions to install the application on Windows Servers.

---

## NOTE

If you are upgrading from a previous version of EFCM, SANavigator, HAFM, or SAN Manager, refer to the *EFCM Upgrade Instructions*.

---

## Pre-Installation

To avoid errors, close all instances of the application before beginning the installation or uninstallation procedures.

## Installation

1. Insert the installation CD into the CD-ROM drive.  
If autorun is enabled, the installer will begin automatically.  
If autorun is not enabled, open the following file:  
`<CD drive>\EFCM97_win\install.exe`
2. On the Introduction screen, click **Next**.
3. On the **Choose Install Set** screen, select **Server and Client** or **Client** and click **Next**.  
**NOTE:** If you select **Client**, the installer will skip the steps that are not required.
4. On the **Select Install Folder** screen, select the usual location for your system's application files (for example, C:\Program Files) and click **Next**.  
**NOTE:** Do not select the installation folder for the previous version.  
**NOTE:** Do not install to the root directory (for example, C:\).
5. On the **Pre-Installation Summary** screen, review the displayed installation summary and click **Install**.
6. On the **Installation Complete** screen, make sure the **Launch EFCM Configuration** check box is selected (default), and click **Done**.

# 1 Installing the Application

The **EFCM 9.7 Configuration** screen displays.

7. On the **Welcome** screen, click **Next**.
8. On the **License Agreement** screen, read the agreement, select **Yes** and click **Next**.
9. On the **Copy Data and Settings** screen, click **No** and then click **Next**.

**NOTE:** To migrate data from a previous version, refer to the *EFCM Upgrade Instructions*.

10. On the **EFCM 9.7 Server Name** screen, enter a name for the Server, and click **Next**.
11. On the **EFCM 9.7 Server License** screen, enter the serial number (on the CD jewel case) and license key (on the Key Certificate), and click **Next**.

The **License Key** field is not case-sensitive.

A message displays that states, configuration is about to start the server, make sure that the **Administrative Tools - Services** window is closed or the server may not start.

12. Click **OK** to close the message.

The **EFCM 9.7 Log In** dialog box displays.

13. In the **User ID** and **Password** fields, enter your user ID and password.

The defaults are Administrator and password, respectively. If you are upgrading from a previous release, your username and password do not change.

14. Click **Login**.
15. Click **OK** on the **EFCM Login Banner**.

For the latest information about this release, refer to the software release notes. Go to the <http://www.brocade.com/support/resources> website and follow the instructions to access the *Brocade EFCM 9.7 Release Notes*.

## Post-Installation Requirements

If you are running in a dual NIC environment, make sure that the Server and FTP Server IP addresses are correct. To edit the Server and FTP Server IP address parameters, complete the following steps.

1. Open the `<Install_Home>\resources\Server\config.properties` file using a text editor (for example, Notepad).

2. Go to the following line:

```
smp.switchToServerIPAddress=
```

3. Enter the IP address of the Server.

4. Save and close the file.

5. Open the `<Install_Home>\ftpServer\apps\ftp\conf\ftpd.conf` file using a text editor (for example, Notepad).

6. Go to the following line:

```
#FtpServer.server.config.host=0.0.0.0
```

(where 0.0.0.0 is the current Server IP address).

7. Change the IP address.

8. Uncomment the `FtpServer.server.config.host` parameter (delete the #).

9. Save and close the file.

10. Stop and restart the server and the FTP server.

## Installing on UNIX Systems

Follow these instructions to install the application on UNIX Servers.

### NOTE

If you are upgrading from a previous version of EFCM, SANavigator, HAFM, or SAN Manager, refer to the *EFCM Upgrade Instructions*.

### Pre-Installation

- To avoid errors, close all instances of the application before beginning the installation or uninstallation procedures.  
If you still receive error messages after closing the application, enter the following commands:  

```
#ps -ef | grep -i ""
```

  
lists the process ID  

```
#kill -9 "process ID"
```
- Check for and install the latest patches for your operating system. For the web sites listing patch information, refer to [Table 12](#).

**TABLE 12** Operating System Patch Information Locations

Platform	URL for Patch Information
Solaris	<a href="http://java.sun.com/j2se/1.4.2/download.html">http://java.sun.com/j2se/1.4.2/download.html</a>

- (Solaris only) To use IPv6 on a server that is IPv4 and IPv6 enabled, complete the following steps.
  - Open a command window.
  - Type `ifconfig <interface name> inet6 plumb up` and press **Enter**.
  - Restart the SAN Management server and client, if running.

If the IPv6 address is not configured properly, the client will show a "Server Not Available at port 51511" message even though the server started successfully.
- Make sure that an X Server is available for display and is configured to permit X Client applications to display from the host on which they are installing the EFCM Server (typically, this simply requires that the systems console be present and running with a logged in user on the X Server based desktop session, such as KDE, GNOME, and so on).  
**NOTE:** If this is a headless unit with no console, refer to ["Headless Pre-Installation Requirements"](#) on page 18.
- Make sure that the DISPLAY environment variable is correctly defined in the shell with a valid value (for example, to display to the local console, `export DISPLAY=:0.0`, or to display to a remote system that has an X Server running, `export DISPLAY=remoteipaddress:0.0`).  
You may also need to consider a firewall that might block the display to the X Server which listens by default on TCP port 6000 on the remote host.

To display to a remote system you need to permit the remote display of the X Server by running command `xhost +IP`, where IP is the IP address of the EFCM server host from the X based desktop of the remote system.

- Make sure to test the DISPLAY definition by running the command `xterm`, from the same shell from which you run `install.bin`. A new X terminal window to the destination X Server display should open.

## Installation

1. Insert the installation CD into the CD-ROM drive and open the following file.  
`<CD_drive>\<UNIX_Platform>\install.bin`
2. On the **Choose Install Set** screen, select **Server and Client** or **Client** and click **Next**.  
**NOTE:** If you select **Client**, the installer will skip the steps that are not required.
3. On the **Select Install Folder** screen, select the usual location for your system's application files (for example, `/opt/EFCM97`) and click **Next**.  
**NOTE:** Do not select the installation folder for the previous version.
4. On the **Pre-Installation Summary** screen, review your installation settings and click **Install**.
5. On the **Installation Complete** screen, make sure the **Launch EFCM Configuration** check box is selected (default), and click **Done**.  
The Configuration screen displays.
6. On the **Welcome** screen, click **Next**.
7. On the **License** screen, read the agreement, select **Yes** and click **Next**.
8. On the **Copy Data and Settings** screen, click **No** and then click **Next**.  
**NOTE:** To migrate data from a previous version, refer to the *EFCM Upgrade Instructions*.
9. On the **EFCM 9.7 Server Name** screen, enter a name for the Server, and click **Next**.
10. On the **EFCM 9.7 Server License** screen, enter the serial number (on the CD jewel case) and license key (on the Key Certificate), and click **Next**.  
The **License Key** field is not case-sensitive.
11. On the **EFCM 9.7 Server License Summary** screen, review to make sure you have the correct configuration and license and click **Finish**.  
The **EFCM 9.7 Log In** dialog box displays.
12. In the **User ID** and **Password** fields, enter your user ID and password.
13. Click **Login**.
14. Click **OK** on the **EFCM Login Banner** screen.

For the latest information about this release, refer to the software release notes. Go to the <http://www.brocade.com/support/resources> website and follow the instructions to access the *Brocade EFCM 9.7 Release Notes*.

## Post-Installation Requirements

On many Unix servers, the X DISPLAY may not always remain available (for example, if you log out of the desktop); therefore, we recommend that you modify the following parameter for the EFCM Server.

To support the EFCM server running when the X DISPLAY is not available (headless mode), complete the following steps (in the `<Install_Home>/bin` directory).

---

### NOTE

If you do not complete these steps, server java errors can occur in functions such as discovery and performance.

---

1. Execute `./EFCM_mgr stop`.
2. Open the `ServerParameters.properties` file and insert the following parameter.  

```
parameter java.awt.headless=true
```
3. Execute `nohup ./EFCM_mgr start`.

## Headless Installation on UNIX Systems

### Headless Pre-Installation Requirements

An X Server display is required, even when performing a headless installation, to run the initial configuration. Before you install EFCM, complete the following:

- Make sure that an X Server is available for display and is configured to permit X Client applications to display from the host on which they are installing the EFCM Connectrix Manager Server (typically, this simply requires that the systems console be present and running with a logged in user on the X Server based desktop session, such as KDE, GNOME, and so on).

The Display can be any host X Server (for example, DISPLAY can be set to display configuration to another UNIX system that has an X based desktop).

- Make sure that the DISPLAY environment variable is correctly defined in the shell with a valid value (for example, to display to the local console, `export DISPLAY=:0.0`, or to display to a remote system that has an X Server running, `export DISPLAY=remoteipaddress:0.0`).

To display to a remote system you need to permit the remote display of the X Server by running command `xhost +IP`, where IP is the IP address of the EFCM server host, on a local terminal window of the X based desktop of the remote system.

You may also need to consider a firewall that might block the display to the X Server which listens by default on TCP port 6000 on the remote host.

To display to a remote system you need to permit the remote display of the X Server by running command `xhost +IP`, where IP is the IP address of the EFCM server host from the X based desktop of the remote system.

- Make sure to test the DISPLAY definition by running the command `xterm`, from the same shell from which you run `install.bin`. A new X terminal window to the destination X Server display should open.

## Headless Installation

To perform a headless installation through the CLI, complete the following steps.

1. Insert the installation CD into the CD ROM drive and open the following file.  
`<CD drive>\<Unix_Platform>\install.bin -i console`  
The installation starts in CLI mode.
2. Choose from the following install sets, and press **Enter**.  
1 - Server and Client  
2 - Client
3. Type the installation folder path and press **Enter**, if necessary.  
To accept the default installation path press **Enter**.  
The pre-Installation summary displays.
4. Review the installation settings and press **Enter** to continue.  
The application is installed.
5. After installation is complete, type 1 and press **Enter** to run Configuration or press **Enter** to run Configuration later.  
Installation Complete message displays.
6. Press **Enter** to complete the installation.
7. To support headless mode correctly, complete the following steps (in the `<Install_Home>/bin` directory).  
**NOTE:** If you do not complete these steps, server java errors can occur in functions such as discovery and performance.
  - a. Execute `./EFCM_mgr stop`.
  - b. Open the `ServerParameters.properties` file and insert the parameter `java.awt.headless=true`.
  - c. Execute `nohup ./EFCM_mgr start`.

## Linux Installation Troubleshooting

If you have completed all of the Linux Pre-Installation requirements and you are still unable to install the application, run the following commands on the host.

1. Go to `<Install_Home>/` (the directory containing `install.bin`).
2. Execute `strace -f -F -v -s 1024 -o efcm9install.txt ./install.bin`.
3. Execute `rpm -qa >> system.txt`.
4. Execute `ps -elf >> system.txt`.
5. Execute `md5sum install.bin >> system.txt`.
6. Execute `df -k >> system.txt`.
7. Execute `sh -c "xterm -e echo nothing >> system.txt 2>&1"`.
8. Execute `env >> system.txt`.
9. Execute `sh -c "DISPLAY=:0.0 xterm -e echo nothing >> system.txt 2>&1"`.
10. Execute `zip support1.zip efcm9install.txt system.txt`.

Send the support1.zip file output from the above (containing `efcm9install.txt` and `system.txt`) to Technical Support. This will assist us in isolating the issue.

# Uninstalling the Application

This section provides step-by-step instructions to uninstall the application from both Windows and UNIX systems.

---

**NOTE**

This version of EFCM is installed on a separate directory from your previous version; therefore, you do not have to uninstall the previous version immediately. However, you cannot run both versions simultaneously.

---

## Uninstalling from Windows Systems

Follow these instructions to uninstall the application from your Windows system.

1. Select **Start > Programs > EFCM 9.7 > Uninstall EFCM**.

If any related services (such as Client.exe or ClientD.exe) are still running, the following Warning message displays: *"Uninstall will stop all the EFCM services and shut down the application if it is running. Do you want to proceed?"*. Click **Yes** to close all services and continue uninstall.

2. On the **Uninstall Option** screen, select one of the following options:
  - **Partial Uninstall**—Configuration and performance data is retained to be re-used by the new installation.
  - **Full Uninstall**—All data is removed.
3. Click **Uninstall**.
4. On the **Uninstall Complete** screen, click **Done**.

## Uninstalling from UNIX Systems

1. Go to `<Install_Home>/Uninstall_EFCM_9.7`.
2. Execute `./Uninstall_EFCM_9.7`.
3. On the **Uninstall Option** screen, select one of the following options:
  - **Partial Uninstall**—Configuration and performance data is retained to be re-used by the new installation.
  - **Full Uninstall**—All data is removed.
4. Click **Uninstall**.
5. On the **Uninstall Complete** screen, click **Done**.

# 1 Uninstalling the Application

## Headless Uninstall from UNIX Systems

If the application was installed using the headless installation, complete the following steps to uninstall.

1. Go to `<Install_Home>/Uninstall_EFCM_9.7`.
2. Execute `./Uninstall_EFCM_9.7 -i console`.
3. Choose from the following install sets, and press **Enter**.
  - 1 - partial Uninstall (Configuration and performance data is retained to be re-used by the new installation.)
  - 2 - full Uninstall in the Terminal (All data is removed.)

# Starting the Application

Follow these instructions to start the application.

## Starting EFCM on Windows Systems

Only use this procedure if you do not want to migrate data from the previous version of the SAN Management application. To migrate data from a previous version, refer to the EFCM Upgrade Instructions.

1. Select **Start > Program Files > EFCM 9.7 > EFCM 9.7** or double-click the desktop icon.

The first time you start the application, a configuration screen displays (if you did not complete configuration during installation).

If this is not the first time you start the application, go to step 9.

2. On the **Welcome** screen, click **Next**.
3. On the **License** screen, read the agreement, select **Yes** and click **Next**.
4. On the **Copy Data and Settings** screen, click **No** and then click **Next**.
5. On the **EFCM 9.7 Server Name** screen, enter a name for the Server, and click **Next**.
6. On the **EFCM 9.7 Server License** screen, enter the serial number (on the CD jewel case) and license key (on the Key Certificate), and click **Next**.  
The **License Key** field is not case-sensitive.
7. On the **EFCM 9.7 Server License Summary** screen, click **Finish**.  
A message displays that states, configuration is about the start the server, make sure that the **Administrative Tools - Services** window is closed or the server may not start.
8. Click **OK** to close the message.
9. On the **EFCM 9.7 Log In** dialog box, enter your user ID and password and click **Login**.
10. Click **OK** on the **EFCM Login Banner**.  
Review the Software Release Notes document.
11. Set up the application to discover a SAN using the instructions in [“Setting Up Discovery”](#) on page 139.

## Starting EFCM on UNIX Systems

Only use this procedure if you do not want to migrate data from the previous version of the SAN Management application. To migrate data from a previous version, refer to the *EFC Manager Software Upgrade Instructions*.

Follow these instructions to start SAN Management application on UNIX systems.

1. To start EFCM 9.7, execute: `nohup ./EFCM_Mgr start` (from the `<Install_Home>/bin` directory where by default `<Install_Home>` is `/opt/EFCM97`).

If this is not the first time you start the application, go to step 9.

2. On the **Welcome** screen, click **Next**.
3. On the **License** screen, read the agreement, click **Yes**, then click **Next**.
4. On the **Copy Data and Settings** screen, click **No**, then click **Next**.
5. On the **EFCM 9.7 Server Name** screen, enter the name to assign the Server, then click **Next**.
6. On the **EFCM 9.7 Server License** screen, enter your product's serial number (on the CD jewel case) and your license key (on the Key Certificate) and click **Next**.
7. On the **EFCM 9.7 Server License Summary** screen, verify the install data, then click **Finish**.

A message displays that states, configuration is about the start the server, make sure that the **Administrative Tools - Services** window is closed or the server may not start.

8. Click **OK** to close the message.
9. On the **EFCM 9.7 Log In** dialog box, enter your user ID and password and click **Login**.
10. Click **OK** on the **EFCM Login Banner**.

Review the Software Release Notes document.

11. Set up the application to discover a SAN using the instructions in ["Setting Up Discovery"](#) on page 139.

# Backing Up and Restoring Data

The SAN Management application helps you to protect your SAN data by backing it up automatically. The data can then be restored, as necessary.

---

**NOTE**

Backing up data takes some time. It is possible that, in a disaster recovery situation, configuration changes made after the last backup interval will be missing from the backup.

---

The SAN Management application allows you to view the backup status at a glance, initiate immediate backup, enable or disable automatic backup, reconfigure the backup directory, interval, and start time, and retrieve backup events.

## What is Backed Up?

The backed up data is contained in the following directories:

- <Install\_Home>\Call Home
- <Install\_Home>\Client
- <Install\_Home>\Resources
- <Install\_Home>\Server

---

**NOTE**

<Install\_Home> refers to the directory where the SAN Management application is installed.

---

The data in those directories is automatically backed up to disk. The data includes the following items:

- All data saved through the Export function.
- All log files.
- All plans saved through the Planning function.
- All reports generated.
- Application configuration data.
- Backup configuration.
- Call home configuration (including phone numbers and dialing options). Note that call home information may be different, depending on which call home centers you use.
- Call home 'Enabled' status of each call home center.
- Call home mapping between call home centers and devices.
- Call home mapping between devices and assigned event filters.
- License information.
- Performance data.
- User-defined sounds.
- User-launched scripts.
- Zoning library (all zone sets and zone definitions) saved through the Zoning function.

## Management Server Backup

There are three options for backing up data to the management server:

- [Configuring Backup to a Writable CD](#)
- [Configuring Backup to a Hard Drive](#)
- [Configuring Backup to a Network Drive](#)

The rack-mount Management Server is backed up to a rewritable (CD-RW) compact disk by default. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the SAN Management application is automatically backed up to the CD-RW when the data directory contents change or when you restart the SAN Management application.

Note that backing up to CD is not the recommended method. The usable capacity of a CD is approximately 700 MB and needs to be replaced when full. Also, CD media has a limited number of re-writes before the medium is exhausted, and write errors occur. It is recommended that you configure the backup system to target a hard drive or a network drive as described in the procedures below.

## Back Up Directory Structure Overview

EFCM backs up data to two alternate folders. For example, if the backup directory location is D:\Backup, the backup service alternates between two backup directories, D:\Backup and D:\BackupAlt. The current backup is always D:\Backup and contains a complete backup of the system. The older backup is always D:\BackupAlt.

If a backup cycle fails, the cause is usually a full CD-RW. When the backup cycle fails, there may only be one directory, D:\Backup. There may also be a D:\BackupTemp directory. Ignore this directory because it may be incomplete.

## Configuring Backup to a Writable CD

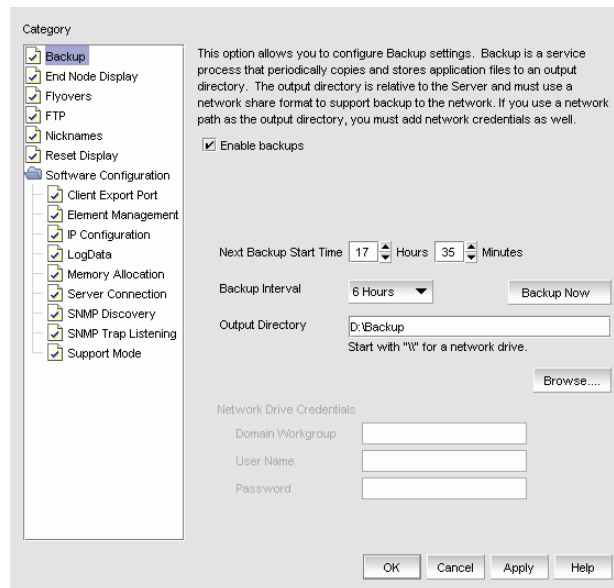
### NOTE

This is not recommended on a permanent basis. CDs have a limited life, and may only last a month. An error message occurs if your SAN Management application can no longer back up to the disc.

To configure the backup function to a writable CD, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays (Figure 2).



**FIGURE 2** Options Dialog Box

2. Select **Backup** in the **Category** list.
3. Select the **Enable backups** check box, if necessary.
4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want the backup process to begin.
5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
6. Verify that the CD backup directory is correct (default directory is D:\Backup).

It is assumed that drive D is a CD-RW drive.

You can change the directory or use the **Browse** button to select another directory.

# 1 Backing Up and Restoring Data

7. Install the formatted disc into the CD drive.

To back up to a writable CD, you must have CD-writing software installed. The disc must be formatted by the CD-writing software so that it behaves like a drive.

8. Click **Apply** or **OK**.

The application verifies that the backup device exists and that the server can write to it. If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

## Configuring Backup to a Hard Drive

---

### NOTE

This requires a hard drive. The drive should not be the same physical drive on which your Operating System or EFCM is installed.

---

To configure the backup function to a hard drive, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.

The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable** backups check box, if necessary.

4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want the backup process to begin.

5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.

6. Click **Browse** to choose the hard drive and directory to which you want to back up your data.

7. Click **Apply** or **OK**.

The application verifies that the backup device exists and that the server can write to it.

If the device does not exist or is not writable, an error message displays that states you have entered an invalid device. Click **OK** to go back to the Options dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

## Configuring Backup to a Network Drive

To back up to a network drive, your workstation can be either in the same domain or in the same workgroup. However, you must have rights to copy files for the network drive.

---

### NOTE

It is recommended that this configuration be completed on the Local client (the client application running on the Server) so that the backup path and location can be confirmed (step 5).

---

To configure the backup function to a network drive, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.

The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable** backups check box, if necessary.
4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want the backup process to begin.
5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
6. Click **Browse** to choose the network share and directory to which you want to back up your data, or enter the network share and directory path.

**NOTE:** You must specify the directory in a network share format (for example, \\network-name\share-name\directory). Do not use the drive letter format (C:\directory).

7. In the **Domain Workgroup** field, enter the name of the Windows domain or workgroup in which you are defined.

**NOTE:** You must be authorized to write to the network device.

8. In the **User Name** field, enter your Windows login name.
9. In the **Password** field, enter your Windows password.
10. Click **Apply** or **OK**.

The application verifies that the device is accessible and that the server can write to it.

If the device does not exist or you are not authorized to write to the network drive, an error message displays that states you have entered an invalid device path or invalid network credentials. Click **OK** to go back to the Options dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

## Enabling Backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Select the **Enable backups** check box.
4. Click **Apply** or **OK**.

## Disabling Backup





Backup is enabled by default. If you want to stop the backup process, you need to disable backup. To disable the backup function, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Clear the **Enable backups** check box.
4. Click **Apply** or **OK**.

## Viewing the Backup Status

The SAN Management application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the backup function.

**TABLE 13** Backup Icons

Icon	Description
	Backup in Progress—displays the following tooltip: “Backup started at hh:mm:ss, in progress... XX directories are backed up.”
	Countdown to Next Scheduled Backup—displays the following tooltip: “Next backup scheduled at hh:mm:ss.”
	Backup Disabled—displays the following tooltip: “Backup is disabled.”
	Backup Failed—displays the following tooltip: “Backup failed at hh:mm:ss mm/dd/yyyy.”

## Changing the Backup Interval

When the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every six hours (360 minutes) by default. However, you can change the interval at which backup occurs.

---

**ATTENTION**

DO NOT modify the backup.properties file.

---

To change the backup interval, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK**.

The minimum value is 15 minutes and the maximum value is 24 hours.

## Starting Immediate Backup

---

**NOTE**

You must have backup privileges to use the Backup Now function.

---

To start the backup process immediately, complete one of the following procedures:

Using the Backup Icon, right-click the **Backup** icon and select **Backup Now**.

OR

1. Using the **SAN** menu, select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Click **Backup Now**.

The backup process begins immediately. There is no confirmation message.

## Reviewing Backup Events

The Master Log, which displays in the lower left area of the main window, lists the events that occur on the SAN.

If you do not see the Master Log, select **View > All Panels**.

The following backup events appear in the Master Log:

- Backup started
- Backup ended
- Backup error
- Backup Enabled
- Backup Disabled
- User selects Backup Now
- Backup destination change
- Backup interval change
- Backup start time change
- Domain workgroup change
- User name change
- User password change
- User set backup interval to an invalid value in the properties file
- User changed backup interval options in the properties file
- Network share access problem when backup starts or during backup (not when the backup configuration is changed)

## Restoring Data

---

**NOTE**

You cannot restore data from a previous version of the SAN Management application.

---

The backed up data is contained in the following directories:

- <Install\_Home>\Call Home
- <Install\_Home>\Client
- <Install\_Home>\Resources
- <Install\_Home>\Server

---

**NOTE**

<Install\_Home> refers to the directory where the SAN Management application is installed.

---

In a disaster recovery situation, it is possible that configuration changes made less than 45 minutes before Server loss (depending on the backup interval you set) could be missing from the backup.

The data in those directories is automatically backed up and can be restored from your disk, network folder, or CD. The data includes the following items:

- All log files.
- All plans saved through the Planning function.
- All reports generated.
- Application configuration data.
- Backup configuration.
- Call home configuration (including phone numbers and dialing options). Note that call home information may be different, depending on which call home centers you use.
- Call home 'Enabled' status of each call home center.
- Call home mapping between call home centers and devices.
- Call home mapping between devices and assigned event filters.
- License information.
- Performance data.
- User-defined sounds.
- User-launched scripts.
- Zoning library (all zones sets and zone definitions).

## Restoring Data from the Brocade-Supplied Rack Mount Management Server

To restore data to the server platform, follow these instructions.

1. Reinstall the application.  
For step-by-step instructions about installing the application, refer to [“Installing the Application”](#) on page 13.
2. Open the SAN Management application and go through the steps in the configuration.
3. Log back into the application.
4. Stop the SAN Management application Services by selecting **Start > Programs > EFCM 9.7 > Stop Services**.  
A DOS window displays messages of services being shut down.
5. Change the directory to `<Install_Home>/bin/`.
6. Double-click `restore.bat`.  
A DOS window opens.
7. At the Command Prompt, enter the path to the backup source directory and press **Enter**.  
The default is `D:\Backup`.
8. At the Command Prompt, enter the path to the destination directory and press **Enter**.  
The default is `<Install_Home>\`.
9. When you receive the “Restore completed” message, press any key to close the DOS window.
10. Restart the SAN Management application.
11. Log back into the application.
12. Make sure discovery is turned on. If it is not, select **Discover > On**.

## Restoring Data from CD

1. Reinstall the application.  
For step-by-step instructions about installing the application, refer to [“Installing the Application”](#) on page 13.
2. Open the SAN Management application and complete the configuration.
3. Stop the Backup Services.
  - a. Select **Start > Settings > Control Panel > Administrative Tools > Services**.  
The **Services** dialog box displays.
  - b. Right-click **EFCM 9.7 Backup** and select **Stop**.
4. Change the directory to `<Install_Home>/bin/`.
5. Double-click `restore.bat`.  
A DOS window opens.

6. At the Command Prompt, enter the path to the backup source directory and press **Enter**.  
The default is D:\Backup.
7. At the Command Prompt, enter the path to the destination directory and press **Enter**.  
The default is <Install\_Home>\EFCM 9.7.
8. When you receive the “Restore completed” message, press any key to close the DOS window.
9. Restart the SAN Management application.
10. Log back into the application.
11. Make sure discovery is turned on. If it is not, select **Discover > On**.

## Restoring Data from the Hard Drive

1. Reinstall the application.  
For step-by-step instructions about installing the application, refer to [“Installing the Application”](#) on page 13.
2. Open the SAN Management application and complete the configuration.
3. Stop the Backup Services.
  - a. Select **Start > Settings > Control Panel > Administrative Tools > Services**.  
The **Services** dialog box displays.
  - b. Right-click **EFCM 9.7 Backup** and select **Stop**.
4. Change the directory to <Install\_Home>/bin/.
5. Double-click restore.bat.  
A DOS window opens.
6. At the Command Prompt, enter the path to the backup source directory and press **Enter**.  
The default is <Hard Drive>:\Backup.
7. At the Command Prompt, enter the path to the destination directory and press **Enter**.  
The default is <Install\_Home>EFCM 9.7.
8. When you receive the “Restore completed” message, press any key to close the DOS window.
9. Restart the SAN Management application.
10. Log back into the application.
11. Make sure discovery is turned on. If it is not, select **Discover > On**.

## Restoring Data from a Network Drive

1. Reinstall the application.  
For step-by-step instructions about installing the application, refer to [“Installing the Application”](#) on page 13.
2. Open the SAN Management application and complete the configuration screens.
3. Stop the Backup Services.
  - a. Select **Start > Settings > Control Panel > Administrative Tools > Services**.  
The **Services** dialog box displays.
  - b. Right-click **EFCM 9.7 Backup** and select **Stop**.
4. Change the directory to `<Install_Home>/bin/`.
5. Double-click `restore.bat`.  
A DOS window opens.
6. At the Command Prompt, enter the path to the backup source directory and press **Enter**.  
The default is `<Network Drive>:\Backup`.
7. At the Command Prompt, enter the path to the destination directory and press **Enter**.  
The default is `<Install_Home>EFCM 9.7`.
8. When you receive the “Restore completed” message, press any key to close the DOS window.
9. Restart the SAN Management application.
10. Log back into the application.
11. Make sure discovery is turned on. If it is not, select **Discover > On**.

# Configuring Advanced Call Home

---

## NOTE

Advanced Call Home is supported on Windows systems for all Call Home Centers and is supported on Solaris for the SUN E-mail Call Home Center.

---

## NOTE

Indirectly discovered switches do not display in the **Products List** table of the **Advanced Call Home** dialog box.

---

## NOTE

SAN routers require firmware 5.0 and higher to display in the **Products List** table of the **Advanced Call Home** dialog box.

---

Advanced Call Home notification allows you to configure the Server to automatically send an e-mail or dial-in to a support center to report system problems on specified devices (switches, routers, and directors). If you are upgrading from a previous release, all of your Call Home settings are preserved.

Advanced Call Home supports multiple call home centers which allows you to configure different devices to contact different call home centers. You can assign devices and filters to the call home centers even when the Call Home Service is not running. All configuration changes take effect once the Call Home Service is started. When you make any call home configuration changes or a call home event trigger occurs, the SAN Management application generates an entry to the master log.

You can configure Advanced Call Home for the following Call Home centers:

- Brocade International (Windows only)
- Brocade North America (Windows only)
- EMC (Windows only)
- HP LAN (Windows only)
- HP Modem (Windows only)
- IBM (Windows only)
- IBM E-mail (Windows only)
- SUN E-mail (Windows and Solaris)

Advanced Call Home, using the Event Management feature, allows you to automate tasks that occur when call home event trigger is fired. When a call home event trigger occurs the SAN Management application generates following actions:

- Sends an e-mail to a specified recipient or dials-in to a support center.
- Exports Performance data, SAN files, Zoning data to a designated location.
- Launches the specified application using a script.
- Adds an entry to the master log file and screen display.
- Displays a message to all open Clients.
- Generates a report.
- Sends an SNMP trap containing information about the triggering event to the receiving system.
- Generates an audible alarm.

For more information about Call Home events, refer to [Appendix](#) , page -287. For more information about Event Management, refer to Event Management Online Help or the *Event Management User Manual*.

Advanced Call Home allows you to perform the following tasks:

# 1 Configuring Advanced Call Home

- Assign devices to and remove devices from the call home centers.
- Define filters from the list of events generated by Brocade devices.
- Edit and remove filters available in the Call Home Event Filters table.
- Apply filters to and remove filters from the devices individually or in groups.
- Edit individual call home center parameters to dial a specified phone number or email a specific recipient.
- Enable and disable individual devices from contacting the assigned call home centers.
- Show or hide call home centers on the display.
- Enable and disable call home centers.

## System Requirements

Advanced Call Home requires the following hardware equipment:

- 1U Server (or any Windows Server with an internal / external modem connection)
- Analog telephone

## Showing a Call Home Center

To show a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. Click **Add/Remove Centers** (beneath the **Call Home Centers** table).

The **Call Home Centers** dialog box displays with a predefined list of call home centers.

3. Select the checkboxes of the call home centers you want to display and click **OK**.

The **Advanced Call Home Configuration** dialog box displays with the selected call home center listed in the **Call Home Centers** table.

## Hiding a Call Home Center

To hide a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. Click **Add/Remove Centers** (beneath the **Call Home Centers** table).

The **Call Home Centers** dialog box displays with a predefined list of call home centers.

3. Clear the checkboxes of the call home centers you want to hide and click **OK**.

The **Advanced Call Home Configuration** dialog box displays with only selected call home centers listed in the **Call Home Centers** table.

## Editing a Call Home Center

---

### NOTE

Advanced Call Home is supported on Windows systems for all Call Home Centers and is supported on Solaris for the SUN E-mail Call Home Center.

---

To edit a call home center, select from the following procedures.

- Editing the Brocade International or IBM Call Home Center .....40
- Editing the Brocade North America or HP Modem Call Home Center .....41
- Editing the EMC Call Home Center.....41
- Editing the HP LAN Call Home Center .....42
- Editing the IBM E-mail or SUN E-mail Call Home Center .....42

### Editing the Brocade International or IBM Call Home Center

To edit a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, select the call home center you want to edit.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays.
4. In the **Call Home Centers** list, select **Brocade International** or **IBM**.
5. Select **Enable** to enable this call home center.
6. To set the interval at which to check the call home center, select the **Set the heartbeat interval at \_\_\_ days (1-28)** check box and enter the interval in the field.
7. In the **Call Home Center - Primary Connection** field, enter the primary phone number or extension of the call home center.
8. In the **Call Home Center - Backup Connection** field, enter the backup phone number or extension of the call home center.
9. In the **Local Server - Phone Number** field, enter the phone number or extension of the local server.
10. In the **Local Server - Server ID** field, enter the identification number of the local server.
11. Click **Send Test** to test the phone number.  
The selected call home center must be enabled to test the phone number.
12. Click **OK**.  
The **Advanced Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.
13. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Editing the Brocade North America or HP Modem Call Home Center

To edit a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, select the call home center you want to edit.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays.
4. In the **Call Home Centers** list, select **Brocade North America** or **HP Modem**.
5. Select **Enable** to enable this call home center.
6. In the **Call Home Center - Phone Number** field, enter the phone number or extension of the call home center.
7. In the **Local Server - Phone Number** field, enter the phone number or extension of the local server.
8. Click **Send Test** to test the phone number.  
The selected call home center must be enabled to test the phone number.
9. Click **OK**.  
The **Advanced Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.
10. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Editing the EMC Call Home Center

To edit a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, select the call home center you want to edit.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays.
4. In the **Call Home Centers** list, select **EMC**.
5. Select **Enable** to enable this call home center.
6. To set the interval at which to check the call home center, select the **Set the heartbeat interval at \_\_\_ days (1-28)** check box and enter the interval in the field.
7. In the **Local Server - Phone Number** field, enter the phone number or extension of the local server.
8. In the **Local Server - Server ID** field, enter the identification number of the local server.
9. In the **Local Server - Site Name** field, enter the site name for the local server.
10. Click **Send Test** to test the phone number.  
The selected call home center must be enabled to test the phone number.

# 1 Configuring Advanced Call Home

11. Click **OK**.

The **Advanced Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

12. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Editing the HP LAN Call Home Center

To edit a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Centers** table, select the call home center you want to edit.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays.

4. In the **Call Home Centers** list, select **HP LAN**.
5. Select **Enable** to enable this call home center.
6. In the **Service Gateway** field, enter the IP address of the call home center.
7. Click **Send Test** to test the phone number.

The selected call home center must be enabled to test the phone number.

8. Click **OK**.

The **Advanced Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

9. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Editing the IBM E-mail or SUN E-mail Call Home Center

To edit a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Centers** table, select the call home center you want to edit.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

The **Configure Call Home Center** dialog box displays.

4. In the **Call Home Centers** list, select **IBM E-mail** or **SUN E-mail**.
5. Select **Enable** to enable this call home center.
6. In the **Customer Details - Name** field, enter the customer contact name.
7. In the **Customer Details - Company** field, enter the company name.
8. In the **Customer Details - Phone (Office)** field, enter the phone number of the customer contact.
9. In the **Customer Details - Phone (Mobile)** field, enter the mobile phone number of the customer contact.

10. In the **SMTP Server Settings - Server Name** field, enter the name of the server.
11. In the **SMTP Server Settings - Port** field, enter the port number of the server.
12. In the **SMTP Server Settings - Username** field, enter a username.  
Optional field unless the SMTP server authentication is enabled.
13. In the **SMTP Server Settings - Password** field, enter a password.  
Optional field unless the SMTP server authentication is enabled.
14. In the **E-mail Notification Settings - Reply Address** field, enter the e-mail address for replies.
15. In the **E-mail Notification Settings - Send To Address** field, enter the customer e-mail address.
16. Click **Send Test** to test the phone number.  
The selected call home center must be enabled to test the phone number.
17. Click **OK**.  
The **Advanced Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.
18. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Enabling a Call Home Center

To enable a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, select the **Enable** check box of the call home center you want to enable.
3. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Testing the Call Home Center Connection

Once you add and enable a call home center, you should verify that call home is functional.

To verify call home center functionality, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.
2. Click **Edit Centers** (beneath the **Call Home Centers** table).  
The **Configure Call Home Center** dialog box displays.
3. In the **Call Home Centers** list, select the center you want to edit.
4. Make sure that the **Enabled** check box is selected.
5. Click **Send Test**.

A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

# 1 Configuring Advanced Call Home

6. Click **OK** to close the 'Test Event Sent' message.
7. Click **OK** to close the **Configure Call Home Center** dialog box.
8. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Disabling a Call Home Center

When a call home center is disabled, no devices can send call home events to the call home center. However, the devices and event filters assigned to the disabled call home center are not removed. You can still perform the following actions on a disabled call home center:

- Edit call home center configuration.
- Add devices and event filters to the call home center.

To disable a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Centers** table, clear the **Enable** check box of the call home center you want to disable.

The selected call home center and its devices and event filters become grayed out. However, the call home center is not actually disabled until you save your changes.

3. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

When a device is assigned to the call home center, a confirmation message displays.




4. Click **Yes**.

## Viewing Call Home Status

You can view call home status from the main SAN Management application window or from the **Call Home Notification** dialog box.

The SAN Management application enables you to view the call home status at a glance by providing a call home status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the call home function.

**TABLE 14** Call Home Icons

Icon	Description
	Normal— Displays when call home is enabled on all devices and no filters are applied.
	Degraded— Displays when call home is enabled on all devices and at least one filter is active.
	Disabled— Displays when any of the following conditions are met: <ul style="list-style-type: none"> <li>• At least one device's call home is disabled.</li> <li>• At least one call home center is disabled from <b>Advanced Call Home</b> dialog box.</li> <li>• At least one non-manageable switch is assigned to any call home center.</li> </ul>

To view more detail regarding call home status, click the **Call Home** icon. The **Call Home Notification** dialog box displays the list of devices that have assigned filters or call home disabled.

The following table explains the statuses that may be displayed in the **Call Home Notification** dialog box.

**TABLE 15** Call Home Status

Status	Description
Enabled	The device is manageable, call home is enabled, and a filter is applied.
Disabled	Call home is disabled on at least one device or call home is disabled from the <b>Advanced Call Home</b> dialog box.
Not Manageable	Manageability is lost.

## Assigning a Device to the Call Home Center

Discovered devices (switches, routers, and directors) are not assigned to a corresponding call home center automatically. You must manually assign each device to a call home center before you use call home.

To assign a device or multiple devices to a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Products List** table, select the devices you want to assign to a call home center.

**NOTE:** Indirectly discovered switches do not display in the **Products List** table.

**NOTE:** SAN routers require firmware 5.0 and higher to display in the **Products List** table.

3. In the **Call Home Center** table, select the call home center to which you want to assign the devices.

You can only assign a device to one call home center at a time.

If you do not select a call home center, the selection defaults to the first call home center in the **Call Home Center** table.

If you have made a previous selection on an assigned device or filter and you do not select a call home center, the selection defaults to the previous selection's call home center.

4. Click **>** (right arrow button).

The selected devices display beneath the selected call home center. Devices assigned to a call home center do not display in the **Products List** table.

5. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Removing a Device From a Call Home Center

To remove a device or multiple devices from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Center** table, select the call home center from which you want to remove devices.
3. Select the devices you want to remove from the selected call home center.
4. Click **<** (left arrow button).

A confirmation message displays.

5. Click **OK**.

The selected devices are removed from the call home center and display in the **Products List** table.

6. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Removing All Devices and Filters From a Call Home Center

To remove all devices and filters from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Center** table, select the call home center from which you want to remove devices and filters.
3. Click **<** (left arrow button).

A confirmation message displays.

4. Click **OK**.

All devices assigned to the selected call home center display in the **Products List** table. Any assigned filters are also removed.

5. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Defining an Event Filter

To define an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. Click **Add** beneath the **Call Home Event Filter** table.  
The **Call Home Event Filter** dialog box displays.
3. In the **Name** field, enter a name for the filter.
4. In the **Description** field, enter a name for the description.
5. In the **Available Call Home Event Types** table, select the events you want to include in the filter.  
Click **Select All** to select all event types in the table or select **Unselect All** to clear the selected event types in the table. For more information about Call Home events, refer to [Appendix](#), page -287.
6. Click **OK**.  
The Event Filter name and the description are displayed in the **Advanced Call Home Configuration** dialog box.
7. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Assigning an Event Filter to a Call Home Center

Event filters allow call home center users to log in to a EFCM server and assign specific event filters to the devices. This limits the number of unnecessary or 'acknowledge' events and improves the performance and effectiveness of the call home center.

You can only select one event filter at a time; however, you can assign the same event filter to multiple devices or call home centers. When you assign an event filter to a call home center, the event filter is assigned to all devices in the call home center. For more information about Call Home events, refer to [Appendix](#), page -287.

---

### NOTE

You cannot assign an event filter to call home center that does not contain devices.

---

To assign an event filter to a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Event Filters** table, select the event filters you want to assign.
3. In the **Call Home Centers** table, select the call home centers to which you want to assign the event filter.
4. Click **>** (right arrow button).  
The selected event filters are assigned to the selected call home centers.
5. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Assigning an Event Filter to a Device

To assign an event filters to a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Event Filters** table, select the event filter you want to assign.

For more information about Call Home events, refer to [Appendix](#) , page -287.

3. In the **Call Home Centers** table, select the devices to which you want to assign the event filter.

4. Click > (right arrow button).

The selected event filters are assigned to the selected devices. The event filter displays beneath the specified device or all of the device under the specified call home center.

5. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Overwriting an Assigned Event Filter

A device can only have one event filter at a time; therefore, when a new filter is applied to a device that already has a filter, you must confirm the new filter assignment.

To overwrite an event filter, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Event Filters** table, select the event filter you want to apply.

For more information about Call Home events, refer to [Appendix](#) , page -287.

3. In the **Call Home Centers** table, select the devices to which you want to apply the event filter.

4. Click > (right arrow button).

For existing event filters, a confirmation messages displays.

5. Click **Yes**.

The selected event filters are applied to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified call home center.

6. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Removing an Event Filter from a Call Home Center

To remove all event filters from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, choose one of the following:
  - Right-click a call home center and select **Remove Filters**.
  - Select the call home center and click < (left arrow button).  
All event filters assigned to the call home center are removed.
3. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Removing an Event Filter from a Device

To remove all event filters from a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Centers** table, choose one of the following:
  - Right-click an event filter assigned to a device and select **Remove Filter**.
  - Right-click a device to which the event filter is assigned and select **Remove Filter**.
  - Select an event filter assigned to a device and click < (left arrow button). Press **CTRL** and click to select multiple event filters assigned to multiple devices.  
All event filters assigned to the device are removed.
3. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Removing an Event Filter from the Call Home Event Filters Table

1. Select **Monitor > Event Notification > Advanced Call Home**.  
The **Advanced Call Home Configuration** dialog box displays.
2. In the **Call Home Event Filters** table, select the event filter you want to remove.
3. Click **Remove**.
  - If the event filter is not assigned to any devices, a confirmation message displays asking if you want to remove the event filter, click **Yes**.
  - If the event filter is assigned to any devices, a confirmation message displays informing you that removing this event filter will remove it from all associated devices, click **Yes**.  
The event filter is removed from any associated devices and the **Call Home Event Filters** table.  
To determine to which devices the event filter is assigned, select the event filter then click > (find button).
4. Click **OK** to close the **Advanced Call Home Configuration** dialog box.

## Searching for an Assigned Event Filter

To find all devices to which that an event filter is assigned, complete the following steps.

1. Select **Monitor > Event Notification > Advanced Call Home**.

The **Advanced Call Home Configuration** dialog box displays.

2. In the **Call Home Event Filters** table, select the event filter you want to find.
3. Click > (find button).
4. All instances of the event filter are highlighted in the **Call Home Centers** table.

If the selected event filter is not assigned to any devices in the call home centers table, a not found message displays.

## Miscellaneous

If a web server is running on the PC, such as IIS, then the default embedded http server port needs to be configured for another port by adding the following property to the <Install\_Home>\resources\server\Config.properties file:

Smp.server.httpserverport=<port number>

## Multiple Network Interface Cards

A second Ethernet NIC card may be desirable in the PC to isolate the switches in your SAN from the public network. If there are any connection issues with the dual NICs, modify the configuration file (<Install\_Home>\resources\Server\config.properties) to force the server to look at a specific IP address. To force the server to look at a specific IP address, add the following parameter to the file:

ServerRmIpAddress=xxx.xxx.xxx.xxx

where xxx.xxx.xxx.xxx is the IP of the NIC card on which you want the client connections to come in.

## Closing the Application

---

### NOTE

Only a controlled application shutdown guarantees the last 10 minutes of data entry. Do not enter any data into the application 10 minutes prior to shutdown.

---

To close the SAN Management Client, select **SAN > Exit**.

To close the SAN Management Client and Server, select **SAN > Shutdown**.

## Using the Documentation

The SAN Management application ships documentation in both PDF format and Online Help. The PDF documentation is shipped on a separate documentation CD-ROM. The Online Help system is part of the SAN Management application and allows you to search all topics to find a particular word or phrase. You can also print help topics as needed.

### Searching the Online Help

To find all the help topics that contain a particular word or phrase, follow these steps.

1. On the **Help** window, click the tab with the magnifying glass icon.
2. In the **Find** field, enter the word or phrase for which you want to search.
3. Press **Enter**.

If any matches are found, a list of topics displays in the panel. The number of times the word or phrase occurs in the topic displays next to the name. Click the name to display that topic.

### Printing an Online Help Topic

To print a help topic, follow these steps.

1. On the **Help** window, click the print icon.  
The **Print** dialog box displays.
2. Select your printer settings and click **OK**.

# Software Overview

---

## In this Chapter

This chapter provides an overview of the user interface.

- The Life Cycle of a SAN .....54
- User Interface Description .....55

## The Life Cycle of a SAN

The application enables you to proceed through the managed life cycle of the SAN with confidence.



**FIGURE 3** The Life Cycle of a SAN

The first stage of a SAN's life cycle is to **Plan the SAN**. Use paper and pen or a software application to plan the SAN.

The second stage of the life cycle is to **Discover the SAN**. The SAN Management application establishes contact with many SAN devices, gathers embedded information, and then depicts it in the Physical Map, or topology. The application discovers the devices attached to the SAN and presents an intuitive visual map of devices and their connections.

The third stage of the life cycle is to **Configure the SAN**, during which you configure SAN devices and fabrics.

The final and longest stage of the life cycle is to **Monitor the SAN**. The application generates events and messages about product and property status. The user interface features an animated display of the data flow and error rates over the entire topology. The application's self-monitoring, event-logging, and event notification features allow you to stay informed about the state of the SAN.

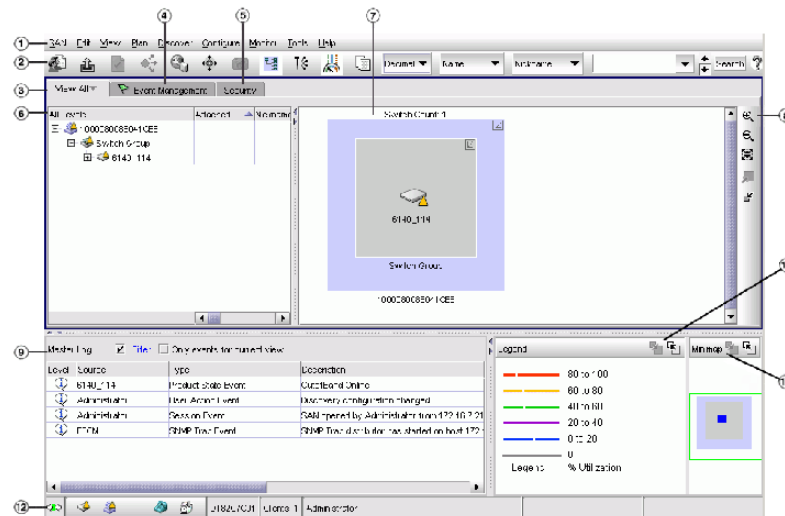
At any point, a discovered SAN can be used as a starting point to plan a new SAN, completing the life cycle.

# User Interface Description

The main window contains a number of areas. Descriptions are listed below the graphic.

## NOTE

Some panels may be hidden by default. To view all panels, select **View > Show Panels > All Panels**, or press **F12**.



**FIGURE 4** Main Window

1. **Menu Bar.** Lists commands you can perform on the SAN.
2. **Toolbar.** Provides buttons that enable quick access to dialog boxes and functions. The buttons vary with the licensed modules on your system.
3. **View tab.** Displays the Master Log, Utilization Legend, Minimap, Physical Map (topology), and Product List. For more information refer to [View Tab](#).
4. **Event Management tab.** Displays the tools you need to automate tasks performed on the SAN. You can configure the application to perform any of the following functions automatically:

- Sending an e-mail message when events or errors occur
- Exporting data
- Playing sound to notify you of specific events

For more information, refer to the *Event Management User Manual*.

5. **Security tab.** Displays the tools you need to manage the authentication settings of all SANtegrity-capable switches and directors in the installation. For more information, refer to the *Security Software User Manual*.
6. **Product List.** Lists the devices discovered in the SAN.
7. **Topology / Physical Map.** Displays the SAN topology, including discovered and monitored devices and connections.
8. **Toolbox.** Provides tools for viewing the Physical Map.
9. **Master Log.** Displays all events that have occurred on the SAN.

10. **Utilization Legend.** Indicates the percentage ranges represented by the colored, dashed lines on the Physical Map.
11. **Minimap.** Displays a “bird’s-eye” view of the entire SAN.
12. **Status Bar.** Displays data regarding the Server, connection, device, and fabric.

### View Tab

The **View** tab displays the Master Log, Utilization Legend, Minimap, Physical Map (topology), and Product List.

To open all areas of the **View** window, select **View > Show Panels > All Panels** or press **F12**.

You can change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

### Product List

The Product List, located on the **View** tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses.

To display the Product List, select **View > Show Panels > Product List** or press **F9**.

---

#### NOTE

Nicknames of attached end-nodes also display in the Product List.

---

You can edit information in the Product List by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

The following columns (in alphabetical order) are included in the Product List.

- **Active FC4 Types.** Displays the active Fibre Channel 4 types of the port.
- **Address.** Displays the address of the port.
- **Alert.** Displays any alerts on the product.
- **All Levels.** Displays all discovered fabrics, groups, devices, and ports.
- **Attached Port #.** Displays the number of the attached port.
- **Block Configuration.** Displays the blocked configuration of the port.
- **Class.** Displays the class to which the product belongs.
- **Class of Service.** Displays the class of service for the port.
- **Comments.** Displays any comments about the product. This field is editable at the fabric and device level.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric and device level.
- **Description.** Displays the description of the product. This field is editable at the fabric and device level.
- **Device Type.** Displays the type of device.
- **Domain ID.** Displays the Domain ID for the product in the format xx(yy), where xx is the Brocade normalized value and yy is the actual value on the wire.
- **Driver.** Displays the product’s driver.
- **Driver Version.** Displays the product’s driver version.
- **Enclosure.** Displays the enclosure of the product. This field is editable at the device level.
- **Fabric.** Displays the fabric nickname of the port.

- **FC Address.** Displays the Fibre Channel address of the port.
- **Firmware.** Displays the firmware version of the product. This field is editable at the device level.
- **IP Address.** Displays the IP address (IPv4 or IPv6 format) of the product. This field is editable at the device level.
- **iSCSI Alias.** Displays the name of the alias target.
- **iSCSI Node Name.** Displays the node name of the product.
- **iSCSI Node Type.** Displays the node type of the product.
- **Location.** Displays the physical location of the product. This field is editable at the fabric and device level.
- **Management Link.** Displays whether the management link for the product is up or down.
- **Max Frame Size (bytes).** Displays the maximum frame size in bytes of the port.
- **Model #.** Displays the model number of the product. This field is editable at the device level.
- **Name (Port).** Displays the name of the port.
- **Name.** Displays the name of the product.
- **Nickname.** Displays the nickname of the product. This field is editable at the fabric, group, and device level.
- **Node WWN.** Displays the node world wide name of the product.
- **Operational State.** Displays the operational state of the port.
- **Operational Status.** Displays the operational status of the product.
- **OS.** Displays the operating system running on the product.
- **OS Device Name.** Displays the device name of the operating system.
- **Port #.** Displays the number of the port.
- **Port Count.** Displays the number of ports on the product.
- **Port Name.** Displays the name of the port.
- **Port Nickname.** Displays any nickname for the port. This field is editable at the port level.
- **Port State.** Displays the state of the port (online or offline).
- **Port Type.** Displays the type of port (for example, expansion port, node port, or NL port).
- **Port WWN.** Displays the world wide name of the port.
- **Receive % Utilization.** Displays the receive percentage utilization of the port.
- **Serial #.** Displays the serial number of the product. This field is editable at the device level.
- **Speed Configured (Gbps).** Displays the actual speed of the port in Gb/s.
- **Speed Supported (Gbps).** Displays the supported speed of the port in Gb/s.
- **State.** Displays the port state.
- **Supported FC4 Types.** Displays the Fibre Channel 4 types supported by the port.
- **Tag #.** Displays the tag number of the product.
- **Text 1 - 4.** Displays user entered information (EFCM 8.X).
- **Transmit % Utilization.** Displays the transmit percentage utilization of the port.
- **Type.** Displays the port type.
- **Vendor.** Displays the name of the product's vendor. This field is editable at the device level.
- **VFID.** Displays the Virtual Fabric ID of the port.

## Master Log

The Master Log, which displays in the lower left area of the main window, lists the events that have occurred on the SAN. If you do not see the Master Log, select **View > Show Panels > All Panels** or press **F5**.

Two daily files are maintained: one that contains events and one that contains summary information. The format of the daily event log file name is *Event\_YYYYMMDD.log*, where YYYYMMDD is the date that the events took place and the log was created. The daily summary file name format is *Event\_YYYYMMDD.sum*.

By default, event history files are kept for 45 days, or until 1000 MB of disk space is used. Log files (and summary files) that are older than 45 days are deleted from the system. In addition, when the total disk space used by all the daily log files exceeds the allowable disk quota, the oldest daily log and the associated summary file are deleted from the system. This check is performed hourly to ensure optimal performance.

The default locations for the log files are  
 <Install\_Home>\Server\Universe\_Home\TestUniverse\\_Working\EventStorageProvider\Event\_YY  
 YMMDD.log and  
 <Install\_Home>\Server\Local\_Root\EventStorageProvider\Event\_YYYYMMDD.sum.




However, you can configure EFCM to archive log files over 45 days old. For step-by-step instructions, refer to [“Archiving Master Log Data”](#) on page 87.

The default locations for the archived log files are <Install\_Home>\savelog\Event\_YYYYMMDD.log and <Install\_Home>\savelog\Event\_YYYYMMDD.sum.

The following fields and columns are included in the Master Log.

- **Level.** The severity of the event. For more information about events, refer to the *Event Management User Manual* or online help. For a list of the events icons, refer to [Table 16](#).

**TABLE 16** Event Icons

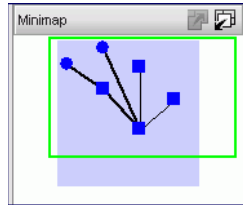
Event Icon	Description
	Informational
	Warning
	Fatal

- **Source.** The product on which the event occurred.
- **Type.** The type of event that occurred (for example, client/server communication events).
- **Description.** A description of the event.
- **Time.** The time and date the event occurred.
- **IP.** The IP address (IPv4 or IPv6 format) of the product on which the event occurred.
- **Node WWN.** The world wide name of the node on which the event occurred.
- **Port WWN.** The world wide name of the port on which the event occurred.

## Minimap

The Minimap, which displays in the lower right corner of the main window, is useful for getting a bird's-eye view of the SAN, or to quickly jump to a specific place on the Physical Map. To jump to a specific location on the Physical Map, click that area on the Minimap. A close-up view of the selected location displays on the Physical Map.

Use the Minimap to view the entire SAN and to navigate more detailed map views. This feature is especially useful if you have a large SAN.



**FIGURE 5** Minimap

## Anchoring or Floating the Minimap

You can anchor or float the Minimap to customize your main window.

### Floating the Minimap

To float the Minimap and view it in a separate window, click the **Detach** icon (📏) in the upper right corner of the Minimap.

### Anchoring the Minimap

To return the Minimap to its original location on the main window, do one of the following steps.

- Click the **Attach** icon (📏) in the upper right corner of the Minimap.
- Click the **Close** icon (✕) in the upper right corner of the Minimap.
- Double-click the logo in the upper left corner of the Minimap.
- Click the logo in the upper left corner of the Minimap and select **Close** (ALT + F4).

## Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.

### Menu Bar

The menu bar is located at the top of the main window. The following lists outline the many functions available on each menu.

**SAN Menu.** The **SAN** menu provides the following commands:

- **Log Out.** Select to log off the SAN Management application.
- **Shutdown.** Select to close the SAN Management Client and Server.
- **Users.** Select to configure users and user groups.
- **Active Sessions.** Select to display all active sessions on the server.
- **Remote Access.** Select to configure remote access.
- **Server Properties.** Select to display the Server properties.
- **Options.** Select to configure the SAN Management application options.
- **Export.** Select to export files.
- **Import.** Select to import files.
- **New Plan.** Select to configure a new planned SAN.
- **Open Plan.** Select to open an existing planned SAN.
- **Save Plan.** Select to save a planned SAN with the same name.
- **Save Plan As.** Select to save a planned SAN with a new name.
- **Exit.** Select to close the SAN Management Client.

**Edit Menu.** The **Edit** menu provides the following commands:

- **Cut.** Select to cut information and move it to another location.
- **Copy.** Select to copy information and move it to another location.
- **Paste.** Select to paste information in another location.
- **Delete.** Select to delete the selected information.
- **Delete All.** Select to delete all information in a specific dialog box.
- **Clear ISL Alert(s).** Select to remove ISL alerts from the selected object.
- **Show Connections.** Select to show connections in a group.
- **Select Connections.** Select to select a connection.
- **Select Attached Devices.** Select to show all devices attached to the selected object.

- **Select Connected Set.** Select to select two connected objects.
- **Select All.** Select to select all object in the physical map.
- **Properties.** Select to display the selected objects properties.

**View Menu.** The **View** menu provides the following commands:

- **Discovered SAN.** Select to display the discovered SAN.
- **Planned SAN.** Select to display a planned SAN.
- **Show Panels.** Select to select which panels to display.
  - **All Panels.** Select to show all panels.
  - **Connectivity Map.** Select to only show the connectivity map.
  - **Product List.** Select to only show the product list.
  - **Event Management.** Select to only show the **Event Management** tab.
  - **Security Center.** Select to only show the **Security** tab.
  - **Master Log.** Select to only show the master log.
- **Manage View.** Select to set up the SAN Management application view.
  - **Create View.** Select to create a new view.
  - **Display View.** Select to display by View All or by a view you create.
  - **Levels.** Select to display by All Levels, Products and Ports, Product Only, or Ports Only.
  - **Copy View.** Select to copy a view.
  - **Delete View.** Select to delete a view.
  - **Edit View.** Select to edit a view.
  - **Connectivity View.** Select to configure a connectivity view.
- **Zoom.** Select to configure the zoom percentage.
- **Show.** Select to determine what products display.
  - **Fabrics Only.** Select to displays only fabrics.
  - **Groups Only.** Select to displays only groups.
  - **All Products.** Select to displays all products.
  - **All Ports.** Select to displays all ports.
- **Enable Flyover Display.** Select to enable flyover display.
- **Show Ports.** Select to show utilized ports on the selected device.
- **Show Connected End Devices.** Select to show all connected end devices.

- **Map Display Layout.** Select to customize a group's layout to make it easier to view the SAN and manage its devices.
  - **Default For Group.** Select to display the devices in the default format.
  - **Custom Grid.** Select to drag and drop device or group icons. Devices can only be moved within a group and groups can only be moved within a fabric. After selecting Custom Grid, click device or a group and drag it to the desired location.
  - **Square.** Select to display the device icons in a square configuration.
  - **Vertical.** Select to display the device icons vertically.
  - **Horizontal.** Select to display the device icons horizontally.
  - **Most Connected at Center.** Select to display the node that has the most connections at the center of the topology.
  - **Directional.** Select to display the internal nodes in a position where they mirror the external groups to which they are connected.
- **Background Color.** Select to customize the topology by changing background color.
  - **Default.** Select to select the default background color.
  - **Custom.** Select to select a background color.
- **Line Types.** Select to determine the way inter-device connections display on the topology.
  - **Straight.** Select to display connections using straight lines.
  - **Orthogonal.** Select to display connections in orthogonal grid lines.
  - **None.** Select to hide the connections between devices.
- **Domain ID/Port #.** Select to set the display domain IDs and port numbers in decimal or hex format.
  - **Decimal.** Select to display all domain IDs and port numbers in decimal format.
  - **Hex.** Select to display all domain IDs in hex format. Port numbers only display in hex format in the Element Managers.
- **Product Label.** Select to configure which product labels display.
  - **Name.** Select to display the product name as the product label.
  - **Nickname.** Select to display the nickname as the product label.
  - **Node WWN.** Select to display the node name as the product label.
  - **IP Address.** Select to display the IP Address (IPv4 or IPv6 format) as the product label.
  - **Domain ID.** Select to display the domain ID as the product label.
- **Port Label.** Select to configure which port labels display.
  - **Nickname.** Select to display the nickname as the port label.
  - **Name.** Select to display the name as the port label.
  - **Port Number.** Select to display the port number as the port label.
  - **Port Address.** Select to display the port address as the port label.
  - **Port WWN.** Select to display the port world wide name as the port label.

- **Port Display.** Select to configure how ports display.
  - **Occupied Product Ports.** Select to display the ports of the devices in the fabrics (present in the physical map) that are connected to other devices.
  - **UnOccupied Product Ports.** Select to display the ports of the devices (shown in the physical map) that are not connected to any other device.
  - **Attached Ports.** Select to display the attached ports of the target devices.
  - **Switch to Switch Connections.** Select to display the switch to switch connections.

**Plan Menu.** The **Plan** menu is only active when you are in the Planned SAN view. To display a planned SAN, select **View > Planned SAN**. The **Plan** menu provides the following commands:

- **Set Rules.** Select to specify planning rules.
- **Evaluate.** Select to evaluate the plan.
- **Insert Devices.** Select to insert a device such as an HBA, bridge, or server.
  - **Multiple Devices.** Select to add multiple devices to your plan.
  - **HBA.** Select to add an HBA device to your plan.
  - **Switch.** Select to add a Switch device to your plan.
  - **Storage.** Select to add a Storage device to your plan.
  - **JBOD.** Select to add a JBOD device to your plan.
  - **Hub.** Select to add a Hub device to your plan.
  - **Bridge.** Select to add a Bridge device to your plan.
  - **Tape.** Select to add a Tape device to your plan.
  - **NAS.** Select to add a NAS device to your plan.
  - **Server.** Select to add a Server device to your plan.
- **Planned Device.** Select to change the selected icon to identify either a planned or an installed device.

**Discover Menu.** The **Discover** menu provides the following commands:

- **On.** Select to turn on Discovery.
- **Off.** Select to turn off Discovery.
- **Setup.** Select to set up Discovery.
- **Servers.** Select to create servers and assign HBAs.
- **Storage Port Mapping.** Select to manually map Storage Ports to a Storage Device or other Storage Ports.
- **Map to Hub.** Select to place each hub in the appropriate location of the topology.

**Configure Menu.** The **Configure** menu provides the following commands:

- **Element Manager.** Select to launch the element manager for a selected device.
- **Group Manager.** Select to manage a group of switches and directors
- **Virtual Switches.** Select to configure virtual switches in the SAN. Virtual switches are created from multiple directors
- **Nicknames.** Select to provide familiar simple names to products and ports in your SAN.
- **SAN Routing.** Select to interconnect storage area network (SAN) islands (separately designated logical portions of a SAN) within a larger network
  - **Router Port Configuration.** Select to view the R\_Ports on a SAN router.
  - **SAN Router Configuration.** Select to configure the Cluster ID, SNMP, Date and Time, SNMP Traps, or iFCP ID for an individual SAN Router or a group of SAN Routers.
  - **Configuration Archive.** Select to archive files and reports, which help customer service troubleshoot problems, as well as configure TFTP root path properties.
  - **Router Consistency.** Select to display the router's properties
  - **Log Viewer.** Select to generate a log file.
  - **Save To Flash.** Select to save changes to the Router Port Configuration or SAN Router Configuration to flash memory.
- **Zoning.** Select to configure zones in SANs.
- **List Zone Members.** Select to display all members in a zone.
- **LUN Management.** Select to configure logical unit numbers (LUNs) for your SANs. LUN Management is an optional module available to previous LUN Management licensed customers.
- **Port Fencing.** Select to configure port fencing to protect your SAN from repeated operational or security problems experienced by ports.
- **Enterprise Fabric Mode.** Select to activate Enterprise Fabric Mode, which enables Fabric Binding, Switch Binding, Domain RSCNs, and Insistent Domain ID.
- **Fabric Binding.** Select to configure whether switches can merge with a selected fabric, which provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

**Monitor Menu.** The **Monitor** menu provides the following commands:

- **Performance.** Select to monitor SAN devices.
  - **Setup.** Select to start performance monitoring.
  - **Latency Graphs.** Select to monitor the time it takes for data to go from an HBA to a device's LUN and back to the HBA.
  - **Switch Graphs.** Select to monitor a switch's performance through a performance graph, which displays transmit and receive data. The graphs show persisted data.
- **View Utilization.** Select to display the connection utilization.
- **Event Notification.** Select to configure the SAN Management application to send event notifications at specified time intervals.
  - **E-mail.** Select to configure the SAN Management application to send event notifications through e-mail.
  - **Advanced Call Home.** Select to configure the SAN Management Server to automatically dial-in to a support center to report system problems.
- **SNMP Agent.** Select to configure the SAN Management application to act as a translator of information stored on the Server into a form usable by SNMP management stations.
  - **On.** Select to turn on SNMP Agent.
  - **Off.** Select to turn off SNMP Agent.
  - **Setup.** Select to configure community strings and trap recipients.
- **Ethernet Event.** Select to configure the application to send notification of Ethernet events.
- **Trap Forwarding.** Select to configure the SAN Management application to send SNMP traps to other computers.
- **Frame Sniffer.** Select to configure the SAN Management application to count frames passed by a switch port that meet user-specified criteria.
- **Reports.** Select to generate reports about the SAN.
  - **Generate.** Select to determine which reports to run.
  - **View.** Select to view reports through the application or through an internet browser.
  - **Consistency.** Select to view the Consistency Report.
  - **iFCP Connections and Zones.** Select to view the iFCP Connections and Zone Report.
  - **LUN Mapping.** Select to view the LUN Mapping Report.
  - **Name Server.** Select to view the Name Server Report.
  - **R Port.** Select to view the R Port Report.
  - **Router Configuration.** Select to view the Router Configuration Report.
  - **Zone Library.** Select to view the Zone Library Report.

- **Logs.** Select to display logs.
  - **Audit.** Select to display a history of user actions performed through the application (except login/logout).
  - **Event.** Select to display errors related to SNMP traps and Client-Server communications.
  - **Fabric.** Select to display the events related to the selected fabric.
  - **Group.** Select to display the event logs defined on the Group Management screen.
  - **Product Status.** Select to display operational status changes of managed products.
  - **Session.** Select to display the users who have logged in and out of the Server.
  - **Security.** Select to display security information.
- **Persist Fabric.** Select to take a “snapshot” of the current products and connections in the fabric as a reference point for comparison to future fabric changes.
- **Unpersist Fabric.** Select to unpersist a fabric.
- **Unpersist Product.** Select to unpersist a single product in a persisted fabric if the product is no longer part of the fabric.
- **Show Route.** Select to view the path that Fibre Channel frames must take between two end-products in a multiswitch fabric.

**NOTE:** Show Route is only available when your Fabric contains two or more Switches.
- **Hide Route.** Select to hide routes that Fibre Channel frames must take between two end-products in a multi-switch fabric.

**Tools Menu.** The **Tools** menu provides the following commands:

- **Setup.** Select to set up the applications that display on the **Tools** menu.
- **Product Menu.** Select to access the tools available on a device’s shortcut menu.
- **Tools (determined by user settings).** Select to open a software application. You can configure the **Tools** menu to display different software applications. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad.

**Help Menu.** The **Help** menu provides the following commands:

- **Contents.** Select to open the Online Help.
- **Find.** Select to search the Online Help.
- **License.** Select to view or change your License information.
- **About EFCM.** Select to view SAN Management application information, such as the release number.

## Toolbar

The toolbar is located at the top of the main window and provides icons to perform various functions (Figure 6).



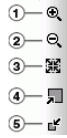
**FIGURE 6** The Toolbar

The buttons on your toolbar will vary based on the licensed features on your system.

1. **Users.** Displays the **EFCM 9.7 Server Users** dialog box. Use to configure users, user groups, and permissions.
2. **Export.** Displays the **Export Discovered SAN** dialog box. Use to export files from a discovered SAN.
3. **Properties.** Displays the **Properties** dialog box of the selected device. Use to view or edit device properties.
4. **Launch Element Manager.** Launches the element manager of the selected device. Use to configure a device through its element manager.
5. **Discover Setup.** Displays the **Discover Setup** dialog box. Use to configure discovery.
6. **Zoning.** Displays the **Zoning** dialog box. Use to configure zoning.
7. **Persist Fabric.** Select to take a “snapshot” of the current products and connections in the fabric as a reference point for comparison to future fabric changes.
8. **Discovered SAN.** Displays the Discovered SAN view when selected from the Planning SAN view.
9. **Planned SAN.** Displays the Planning SAN view when selected from the Discovered SAN view. Use to plan a SAN.
10. **View Utilization.** Displays or hides the utilization legend.
11. **View Report.** Displays the **View Reports** dialog box. Use to view available reports.
12. **Domain ID/Port #.** Use to set the dutchman ID or port number to display as decimal or hex in the physical map.
13. **Product Label.** Use to set the product label for the devices in the physical map.
14. **Port Label.** Use to set the port label for the devices in the physical map.
15. **Search.** Use to search for a device on the physical map and product list.
16. **Help.** Displays the Online Help.

### Toolbox

The toolbox (Figure 7) is located at the top right side of the **View** window and provides tools to zoom in and out of the Physical Map, collapse and expand groups, and fit the topology to the window.



**FIGURE 7** The Toolbox

1. **Zoom In.** Use to zoom in on the Physical Map
2. **Zoom Out.** Use to zoom out on the Physical Map.
3. **Fit in View.** Use to scale the map to fit within the Physical Map area.
4. **Expand.** Use to expand the map to show all ports in use on a device.
5. **Collapse.** Use to collapse the map to show only devices (hides ports).

### Status Bar

The status bar (Figure 8) displays at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar change to reflect different information, such as the current status of products, fabrics, and backup.



**FIGURE 8** Status Bar

The icons on your status bar will vary based on the licensed features on your system.

1. **Connection Status.** Displays the Server-Client connection status.
2. **Product Status.** Displays the status of the most degraded device in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status displays as degraded. Click this icon to open the **Product Status Log**. For more information, refer to [“Determining a Product’s Operational Status”](#) on page 164.
3. **Fabric Status.** Displays the state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded or failed. Select a product or fabric from the Physical Map or Product List and click this button to open the related **Fabric Log** (only available for persisted fabrics). For more information, refer to [“Viewing the Fabric Log”](#) on page 218.
4. **Attention Indicator.** This icon displays when at least one Brocade or IBM product in the SAN requires attention. Click the icon to open the **Service Request** dialog box, which lists all Brocade or IBM switches and directors with an attention indicator.

5. **Call-Home Status.** Displays a call home status icon when one or more fabrics are discovered, which allows you to determine the current call home status. For more information about Advanced Call Home status and icons, refer to [“Viewing Call Home Status”](#) on page 45.
6. **Backup Status.** Displays a backup status icon, which allows you to determine the current backup status. Let the pointer pause on the backup status icon to display the following information in a tooltip.
  - **Backup in Progress icon.** Backup started at hh:mm:ss, in progress... XX files in <directory\_name> are backed up.
  - **Countdown to Next Scheduled Backup icon.** Waiting for next backup to start.
  - **Backup Disabled icon.** Backup is disabled.
  - **Backup Failed icon.** Backup failed at hh:mm:ss mm/dd/yyyy.
7. **Server Name.** Displays the name of the Server to which you are connected.
8. **Total Users.** Displays the number of clients logged into the server.
9. **User's ID.** Displays the user ID of the logged in user.

## 2 User Interface Description

# Setting Up the Application

---

## In this Chapter

This chapter provides instructions for setting up and customizing the application.

- Server and Client Communication Requirements . . . . . 72
- Configuring a Server . . . . . 73
- Configuring the Client . . . . . 79
- Configuration Options . . . . . 79
- Managing Users . . . . . 89
- Managing User Groups . . . . . 94
- Configuring Remote Access . . . . . 100
- Partitioned Switch Support . . . . . 102
- Customizing the Main Window . . . . . 103
- Customizing Device Properties . . . . . 105
- Export and Import . . . . . 109
- Accessing Third-Party Tools . . . . . 123
- Accessing Eclipse Management Applications . . . . . 130

# Server and Client Communication Requirements

The SAN Management application has the following Server and Client communication requirements:

- **IP Connection to Switches** - The SAN Management Server and Client software poll different fabric information directly, requiring access to each switch by way of an IP connection. Make sure that the network environment does not have a proxy server or firewall between the devices and the Server and Clients. If a proxy server or firewall exists, make sure that proper rules are set up to allow access.
- **Port Numbers** - For some SAN Management functions to work correctly the following TCP/UDP port numbers must not be blocked by a proxy server or network firewall:
  - 20,(FTP port)
  - 21 (built-in FTP server port)
  - 23 (telnet/sectelnet port)
  - 162 (SNMP port)
  - 2048, 2049 (MPI discovery ports)
  - 80 (HTTP port)
  - 443 (HTTPS port)
  - 1812, 1813 (RADIUS ports)

If a firewall exists between the Server and Client, the following port numbers must be open:

- 80 (Web Server port number on the Server port)
- 51511 (API-Server to Client communication port)
- 51510 (API-Server to Client export port)
- 55555 (API-Client to Server export port)
- 51513 (ECCAPI port)
- 8081 (Web proxy port)

## Configuring a Server

The application has two parts: the Server and the Client. The Server is installed on one machine and stores SAN-related information; it does not have a user interface. To view SAN information through a user interface, you must log in to the Server through a Client. The Server and Clients may reside on the same machine, or on separate machines.

The server relies on DataFabric Manager to discover the SAN storage devices and hosts. To configure SAN Manager to connect to DataFabric Manager, see [“Configuring the Product Type and Access”](#) on page 149.

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but is immediately logged out because the Server cannot reach the Client. To resolve this issue, the application automatically detects the network configuration and runs the Client in “polling mode” when necessary.

When the Client is not running in polling mode, the Server calls the Client whenever it has new data. When the Client is running in polling mode, the Server queues up the data and the Client periodically checks in (approximately every five or ten seconds) and gets the data.

## Logging In to a Server

You must log into a Server to monitor a SAN.

### NOTE

You must have an established login and password account on the Server to log in.

1. Select **Start > Program Files > EFCM 9.7 > EFCM 9.7** or double-click the desktop icon.

The **EFCM 9.7 Log In** dialog box displays (Figure 9).

**FIGURE 9** Log In Dialog Box

2. Specify a new address by typing it in the **Network Address** field, or selecting one from the list.

**NOTE:** Localhost is the default value. The application automatically determines the local IP address and uses that value as the local host address.

The SAN Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

## 3 Configuring a Server

IPv4 addresses are normally written as four groups of three decimals. For example, 123.023.123.023 is a valid IPv4 address. The SAN Management application accepts the following IPv4 address formats:

- 123.023.123.023 (Complete address including leading zeros.)
- 123.23.123.23 (Compressed format with leading zeros omitted. This is the default display.)

IPv6 addresses are normally written as eight groups of four hexadecimal digits. For example, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 is a valid IPv6 address. The SAN Management application accepts the following IPv6 address formats:

- AAAA:0AAA:0000:AAAA:AAAA:AAAA:AAAA:AAAA (Complete address including leading zeros.)
- AAAA:AAA:0:0:AAAA:AAAA:AAAA:AAAA (Compressed format with leading zeros omitted. This is the default display.)
- AAAA:AAA::AAAA:AAAA:AAAA:AAAA (Compressed format with double colons for successive hexadecimal fields of zeros.)
- <IPv6\_Address>:<Port\_Number> (Any IP IPv6 address format and port number. The default port number is 51511.)

The Server's name displays in the **Server Name** field.

3. Enter your user ID and password.
4. Click **Forget password** or **Save password** to select whether you want the application to remember your password the next time you log in.
5. Click **Login**.

### Changing Your Password

1. Select **Start > Programs > EFCM 9.7 > EFCM 9.7** to open the application.

The **EFCM 9.7 Log In** dialog box displays.

2. Enter your user name in the **User ID** field.
3. Enter your password in the **Password** field.
4. Click **Change**.

The **Change Password** dialog box displays.

5. Enter your new password in the **Secure Password** and **Retype Password** fields and click **OK**.
6. Click **Login**.

### Logging Out of a Server

Select **SAN > Log Out**.

You are logged out of the current Server and the **EFCM 9.7 Log In** dialog box displays. For instructions on logging in to a new Server, refer to [“Logging In to a Server”](#) on page 73.

## Adding a Server

1. Select **SAN > Log Out**.

The **EFCM 9.7 Log In** dialog box displays.

2. Enter the Server's network address in the **Network Address** field.

The SAN Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

IPv4 addresses are normally written as four groups of three decimals. For example, 123.023.123.023 is a valid IPv4 address. The SAN Management application accepts the following IPv4 address formats:

- 123.023.123.023 (Complete address including leading zeros.)
- 123.23.123.23 (Compressed format with leading zeros omitted. This is the default display.)

IPv6 addresses are normally written as eight groups of four hexadecimal digits. For example, 2001:0db8:85a3:08d3:1319:8a2e:0370:7334 is a valid IPv6 address. The SAN Management application accepts the following IPv6 address formats:

- AAAA:0AAA:0000:AAAA:AAAA:AAAA:AAAA:AAAA (Complete address including leading zeros.)
- AAAA:AAA:0:0:AAAA:AAAA:AAAA:AAAA (Compressed format with leading zeros omitted. This is the default display.)
- AAAA:AAA::AAAA:AAAA:AAAA:AAAA (Compressed format with double colons for successive hexadecimal fields of zeros.)
- <IPv6\_Address>:<Port\_Number> (Any IP IPv6 address format and port number. The default port number is 51511.)

**NOTE:** You must have an established login and password account on the new Server.

The Server's name displays in the **Server Name** field.

3. Enter your user ID and password.
4. Click **Forget password** or **Save password** to select whether you want the application to remember your password the next time you log in.
5. Click **Login**.

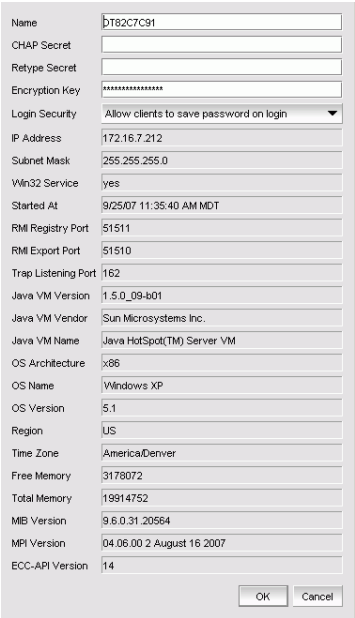
The application logs into the Server located at the specified network address.

### 3 Configuring a Server

## Viewing Server Properties

Select **SAN > Server Properties**.

The **EFCM 9.7 Server Properties** dialog box displays (Figure 12).



The EFCM 9.7 Server Properties dialog box is a configuration window with a list of server parameters and their values. The parameters are listed on the left, and the corresponding values are in text boxes on the right. At the bottom right, there are 'OK' and 'Cancel' buttons.

Name	DT82C7C91
CHAP Secret	
Retype Secret	
Encryption Key	*****
Login Security	Allow clients to save password on login
IP Address	172.16.7.212
Subnet Mask	255.255.255.0
Vm32 Service	yes
Started At	9/25/07 11:35:40 AM MDT
RMI Registry Port	51511
RMI Export Port	51510
Trap Listening Port	162
Java VM Version	1.5.0_09-b01
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) Server VM
OS Architecture	x86
OS Name	Windows XP
OS Version	5.1
Region	US
Time Zone	America/Denver
Free Memory	3178072
Total Memory	19914752
MIB Version	9.6.0.31.20564
MPI Version	04.06.00.2 August 16 2007
ECC-API Version	14

**FIGURE 10** EFCM 9.7 Server Properties dialog box

## Configuring HBAs and Servers

The SAN Management application allows you to associate an HBA to a Server, unassociate an HBA from a Server, rename a Server, and delete a Server.

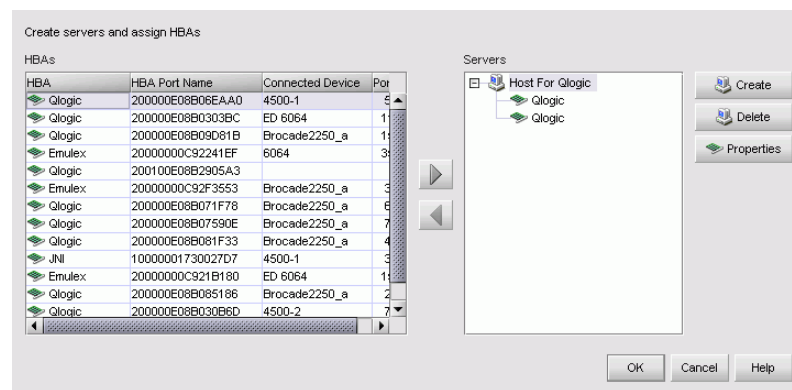
### Associating an HBA to a Server

#### ATTENTION

Discovered information overwrites your user settings.

1. On the Physical Map, right-click an HBA icon and select **Server HBA Mapping** from the menu.

The **Create servers and assign HBAs** dialog box displays (Figure 11).



**FIGURE 11** Create Servers and Assign HBAs Dialog Box

2. In the **Servers** table, select the server to which you want to assign HBAs.

**NOTE:** To add or remove servers, click **Create** or **Delete**. To rename a server click the server name once, wait, then click it again. Type the new name over the old name.

3. Select the HBA from the table on the left and click the right arrow.

The HBA displays in the **Servers** table. The HBA is now associated with the selected server.

4. Click **OK** to save your changes and close the **Create servers and assign HBAs** dialog box.

On the Physical Map, the HBA displays in the server.

### Unassociating an HBA from a Server

1. On the Physical Map, right-click an HBA icon and select **Server HBA Mapping** from the menu.

The **Create servers and assign HBAs** dialog box displays.

2. Select the HBA from the **Servers** table on the right and click the left arrow.

The HBA you selected is removed from the **Servers** table and the HBA is no longer associated with the server.

3. Click **OK** to save your changes and close the **Create servers and assign HBAs** dialog box.

On the Physical Map, the HBA displays on its own.

### Renaming a Server

You can rename Servers that display on the Physical Map.

1. On the Physical Map, right-click an HBA icon and select **Server HBA Mapping** from the menu.  
The **Create servers and assign HBAs** dialog box displays.
2. Click once on the Server name in the **Servers** table on the right.
3. Edit the Server name.
4. Press **Enter**.

The Server's new name displays on the Physical Map.

### Deleting a Server

You can delete Servers that display on the Physical Map.

1. On the Physical Map, right-click an HBA icon and select **Server HBA Mapping** from the menu.  
The **Create servers and assign HBAs** dialog box displays.
2. From the **Servers** table on the right, select the Server you want to delete.
3. Click **Delete**.  
The server is deleted.
4. Click **OK** to save your changes and close the **Create servers and assign HBAs** dialog box.

### Removing a Server

You can remove Servers from the list in the **EFCM 9.7 Log In** dialog box.

1. Select **Start > Program Files > EFCM 9.7 > EFCM 9.7** or double-click the desktop icon.  
The **EFCM 9.7 Log In** dialog box displays.
2. From the **Network Address** list, select the Server you want to remove.  
The selected Server's IP address displays in the **Network Address** field.
3. Click **Delete**.  
A confirmation message displays to confirm you want to delete the selected server.
4. Click **OK**.

## Configuring the Client

1. Select **Start > Program Files > EFCM 9.7 > EFCM 9.7** or double-click the desktop icon.  
The **EFCM 9.7 Log In** dialog box displays.
2. Click **Setup**.  
The **Client Setup** dialog box displays.
3. In the **Client Export Port #** field, enter a new TCP port number, if necessary.
4. In the **Memory Allocation** field, enter a new value, if necessary.
5. Click **OK**.

## Configuration Options

EFCM enables you to configure the following options:

- Backup
- End Node Display
- Flyovers
- FTP
- Nicknames
- Reset Display
- Software Configuration

### Configuring Backup Settings

---

**NOTE**

You must have Backup Read/Write privileges to configure Backup settings.

---

To configure backup settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Select the **Enable backups** check box.
4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want the backup process to begin.
5. Select an interval from the **Backup Interval** list to set how often backup occurs.
6. In the **Output Directory** field, enter the path for the backup directory.

**NOTE:** If you set your backup directory to a network drive, you must specify the directory in a share format (for example, \\server\share\). You must also supply user credentials for a user that is authorized to write to the network device.

You can change the directory or use the **Browse** button to select another directory.

7. Set the **Network Drive Credentials**, if necessary.
  - a. In the **Domain or Workgroup** field, enter the domain or workgroup name.
  - b. In the **User Name** field, enter the user name.
  - c. In the **Password** field, enter the password.

8. Click **Apply** or **OK** to save your work.

The application verifies that the backup device exists and that the server can write to it.

If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

Backup occurs, if needed, at the interval you specified.

### Configuring End Node Display

To display end nodes when discovering a new fabric, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **End Node Display**.
3. Select the **Show connected end nodes when new fabric is discovered** check box to display end nodes on your system.

**NOTE:** Before changes can take effect, the topology must be rediscovered.

4. Click **Apply** or **OK** to save your work.

### Configuring Flyover Settings

You can configure your system to display product information for products and connections in a pop-up window on the Physical Map.

To display product information in a pop-up window, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Flyovers**.
3. Select the **Enable flyover display** check box to enable flyover display on your system.
4. Select the **Include labels** check box to include labels on flyover displays.
5. To set the products to display on flyover, select the **Product** tab and complete the following steps.
  - a. In the **Available Properties** table, select each product you want to display.
  - b. Click the right arrow to move the selected products to the **Selected Properties** table.
  - c. Use the **Move Up** and **Move Down** buttons to reorder the products in the **Selected Properties** table, if necessary.

Items in the **Selected Properties** table appear in the flyover display.

6. To set the connections to display on flyover, click the **Connection** tab and complete the following steps.
  - a. In the **Available Properties** table, select all the products you want to display.
  - b. Click the right arrow to move the selected products to the **Selected Properties** table.
  - c. Use the **Move Up** and **Move Down** buttons to reorder the products in the **Selected Properties** table.

Items in the **Selected Properties** table appear in the flyover display.
7. Click Apply or OK to save your work.

## Configuring FTP Server Settings

In EFCM 9.7, a built in FTP server and its services are installed during installation. Other FTP servers on your system are recognized by the application as external FTP servers. For Windows systems, the built in FTP server is the default configuration and installation starts the FTP service if port 21 is not used by any other FTP server. For UNIX systems, the external FTP server is the default. Note that when uninstalling the application the built in FTP server is removed with all other services even if the FTP service is used by firmware upgrade or supportsave features.

To configure the FTP server settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **FTP**.
3. Choose one of the following options:
  - Select the **Use built in FTP Server** option to use the default built in FTP server.
    - a. In the **FTP User Name and Password** list, select **Default** or **User Defined**.  
If you select **Default**, go to [step 4](#). If you select **User Defined**, continue with [step b](#).
    - b. In the **User Name** field, enter your user name.
    - c. In the **Password** and **Confirm Password** fields, enter your password. Go to [step 4](#).
  - Select the **Use External FTP Server** option to configure the external FTP server.
    - a. In the **Remote Host IP** field, enter the IP address for the remote host.
    - b. In the **Remote User Name** field, enter a user name.
    - c. In the **Remote Directory Path** field, enter the path to the remote host.
    - d. In the **Password Required for FTP** field, enter the password.
4. Click **Apply** or **OK** to save your work.

### Configuring Nickname Settings

The SAN Management application allows you to configure nicknames to be either unique or non-unique.

To configure nicknames, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Nicknames**.
3. Select one of the following options.
  - Select **Set nicknames to be unique** to require that nicknames be unique on your system.
  - Select **Set nicknames to be non-unique** to allow duplicate nicknames on your system.
4. Click **Apply** or **OK** to save your work.

### Editing Duplicate Nicknames

The SAN Management application allows you to edit duplicate nicknames so that each device has a unique nickname.

Note that this dialog box only displays when you set nicknames to be unique and there are duplicate nicknames in the system.

To edit duplicate nicknames, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Nicknames**.
3. Select **Set nicknames to be unique** to require that nicknames be unique on your system.
4. Click **OK** on the **Options** dialog box.

The **Duplicated Nicknames** dialog displays.

5. Select one of the following options.
  - If you select **Append Incremental numbers for all repetitive nicknames**, the nicknames are edited automatically using incremental numbering.
  - If you select **I will fix them myself**, edit the nickname in the **Nickname** field.
6. Click **Apply** or **OK** to save your work.

## Configuring Reset Display Settings

You can reset your system to display the following EFCM classic display settings.

**TABLE 17** EFCM Classic Display Settings

Settings	Default State
Show port	Disabled.
Show connected end device	Disabled.
Map Layout	Set to default for Groups.
Line Types	Set to default for Groups.
Port Display	Set to Attached Ports only.
Product Flyover	Set to include the only following properties: Nickname, Name, WWN, IP Address, and Domain ID.
Map Flyovers	Set to include the following properties: Nickname, IP Address, WWN, Port Number Hex, Port Address, and Port WWN.
Master Log Events	Set to hide Extended Events.
Product List	Set to only display basic property list.

To reset EFCM to the default EFCM display and view settings, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Reset Display**.

3. Click **Reset Display**.

4. Click **Yes** on the reset confirmation message.

The display and view settings are immediately reset to the default EFCM classic display settings (as detailed in the [EFCM Classic Display Settings](#) table).

5. Click **Apply** or **OK** to save your work.

### Configuring Software Settings

The SAN Management application allows you to configure the following software settings:

- **Client Export Port**—Configure a port for communication between the client and server.
- **Element Management**—Configure the element management method.
- **IP Configuration**—Configure the Ethernet ports.
- **LogData**—Archive Master log data.
- **Memory Allocation**—Configure memory allocation for the client and server.
- **Server Connection**—Configure client-server connectivity settings.
- **SNMP Discovery**—Configure the SNMP timeout and retry settings.
- **SNMP Trap Listening**—Configure the SNMP Trap port.
- **Support Mode**—Configure support settings to allow enhanced diagnostics.

### Configuring Client Export Port Settings

To configure client export port settings, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Client Export Port** to assign a communications port between the client and server.
3. In the **Client Export Port** field, enter the client export port number to set a fixed port number for the client.
4. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

### Configuring Element Management Settings

To configure element management settings, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Software Configuration**.
3. Select **Element Management**.
4. Choose one of the following options:
  - Select the **SNMP and management discovery** option to allow discovery and monitoring by this server and not allow element management capability from other servers.
  - Select the **SNMP Discovery Only** option to allow discovery and monitoring without overriding the element management capability from another server.
5. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

## Configuring IP Configuration Settings

To configure the IP address and subnet mask to override the default Ethernet ports used by the server for client-server communications, complete the following steps. The SAN Management application enables you to run your server in dual mode, which allows the client to communicate from both IPv4 and IPv6.

---

### NOTE

The server binds using IPv6 address by default if your Operating System is IPv6 enabled (dual mode or IPv6 only). Server binds using IPv4 address by default if your Operating System is IPv4 enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

---

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **IP Configuration** to set the IP address and subnet mask.
3. In the **Server IP Configuration** list, choose from one of the following options.
  - Select **Automatic**. Go to [step 5](#).
  - Select **Manual**. Continue with [step 4](#).
4. In the **Return Address** area, choose from one of the following options.
  - If your operating system has IPv4 only, complete the following steps.
    - a. In the **Subnet Mask** field, enter the subnet mask address for the server.
    - b. In the **Return Address** field, enter the return address for the server. Continue with [step 5](#).
  - If your operating system has IPv6 only, complete the following steps.
    - a. In the **IPv6 Address** field, enter the subnet mask address for the server.
    - b. In the **Prefix Length** field, enter the prefix length. Continue with [step 5](#).
  - If your operating system has IPv4 and IPv6, select one of the following options.
    - If your operating system has **IPv4**, select the **IPv4 Address** option and complete the following steps
      - a. In the **IPv4 Address** field, enter the return address for the server.
      - b. In the **Subnet Mask** field, enter the subnet mask address for the server. Continue with [step 5](#).
    - If your operating system has **IPv6**, select the **IPv6 Address** option and complete the following steps
      - a. In the **IPv6 Address** field, enter the return address for the server.
      - b. In the **Prefix Length** field, enter the prefix length. Continue with [step 5](#).
5. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

### Configuring the Application to Use Dual Network Cards

Issues with Client-to-Server connectivity can be due to different causes. Some examples are:

- The computer running the Server has more than one network interface card (NIC) installed.
- The computer running the Server is behind a firewall that performs network address translation.

To make sure that Clients can connect to the Server, you may need to edit the IP configuration setting in the **Options** dialog to manually specify the IP address that the Server should use to communicate to its Clients.

---

#### NOTE

The server binds using IPv6 address by default if your Operating System is IPv6 enabled (dual mode or IPv6 only). Server binds using IPv4 address by default if your Operating System is IPv4 enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

---

To configure the IP address and subnet mask to override the default RMI server host IP address, complete the following steps.

---

#### NOTE

This configuration option replaces the `-Djava.rmi.server.hostname` value used in previous releases.

---

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **IP Configuration** to set the IP address and subnet mask.
3. In the **Server IP Configuration** list, choose from one of the following options.
  - Select **Automatic**. Go to [step 5](#).
  - Select **Manual**. Continue with [step 4](#).
4. In the **Return Address** area, choose from one of the following options.
  - If your operating system has IPv4 only, complete the following steps.
    - a. In the **Subnet Mask** field, enter the subnet mask address for the server.
    - b. In the **Return Address** field, enter the return address for the server. Continue with [step 5](#).
  - If your operating system has IPv6 only, complete the following steps.
    - a. In the **IPv6 Address** field, enter the subnet mask address for the server.
    - b. In the **Prefix Length** field, enter the prefix length. Continue with [step 5](#).

- If your operating system has IPv4 and IPv6, select one of the following options.
  - If your operating system has **IPv4**, select the **IPv4 Address** option and complete the following steps
    - a. In the **IPv4 Address** field, enter the return address for the server.
    - b. In the **Subnet Mask** field, enter the subnet mask address for the server. Continue with [step 5](#).
  - If your operating system has IPv6, select the **IPv6 Address** option and complete the following steps
    - a. In the **IPv6 Address** field, enter the return address for the server.
    - b. In the **Prefix Length** field, enter the prefix length. Continue with [step 5](#).
- 5. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

## Archiving Master Log Data

To archive master log data, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **LogData**.
3. Select the **Archive master log data** check box.

The master log data is archived to the `<Install_Home>\savelog` directory.

**NOTE:** Changes to this option take effect after an application restart.

4. Click **Apply** or **OK** to save your work.

## Configuring Memory Allocation Settings

To configure memory allocation settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Memory Allocation** to set the memory allocation for the server and client.
3. In the **Client Memory Allocation** field, enter the memory allocation (MB) for the client.
4. In the **Server Memory Allocation** field, enter the memory allocation (MB) for the server.

If your server has a minimum of 2 Gb RAM, change the default server memory value to 1024 MB.

**NOTE:** If your server is running less than 2 Gb RAM, do not change the default (512 MB).

5. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

### Configuring Server Connection Settings

The SAN Management application allows you to configure client-server connectivity settings so that you can assign a server connection port for the initial contact from the client, assign a server export port from communications between server and client, and set the server export port to be SSL-enabled.

To configure server connection settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **Server Connection** to configure client-server connectivity settings.
3. In the **Server Connection Port #** field, enter a port number for the initial contact from the client.
4. In the **Server Export (SSL) Port #** field, enter a port number for communications between the client and the server.
5. Click **Enable SSL** to enable this function for the server export port.
6. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

### Configuring SNMP Discovery Settings

To configure SNMP discovery settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **SNMP Discovery** to set the number of retries and timeout for SNMP discovery between the client and server.
3. In the **SNMP Timeout** field, enter a timeout value (default=5) for discovery between the application and the managed products (switches and directors).
4. In the **SNMP Retry** field, select the number of retries for discovery between the application and the managed products (switches and directors).
5. Select the **Apply settings to all currently defined IP addresses** check box.
6. Click **Apply** or **OK** to save your work.

### Configuring SNMP Trap Listening Settings

To configure SNMP trap listening settings, complete the following steps.

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **SNMP Trap Listening**.
3. In the **SNMP Listening Port** field, enter a SNMP listening port number to assign a port to retrieve SNMP traps.
4. Click **Apply** or **OK** to save your work.

**NOTE:** Changes to this option take effect after an application restart.

## Configuring Support Mode Settings

To configure support mode settings, complete the following steps.

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **Support Modes** to enable or disable support modes.

**NOTE:** Only use this option when directed to by customer support.

3. Select the **Client Support Mode** check box to enable the support mode for the client.
4. Select the **Server Support Mode** check box to enable the support mode for the server.
5. Click **Apply** or **OK** to save your work.

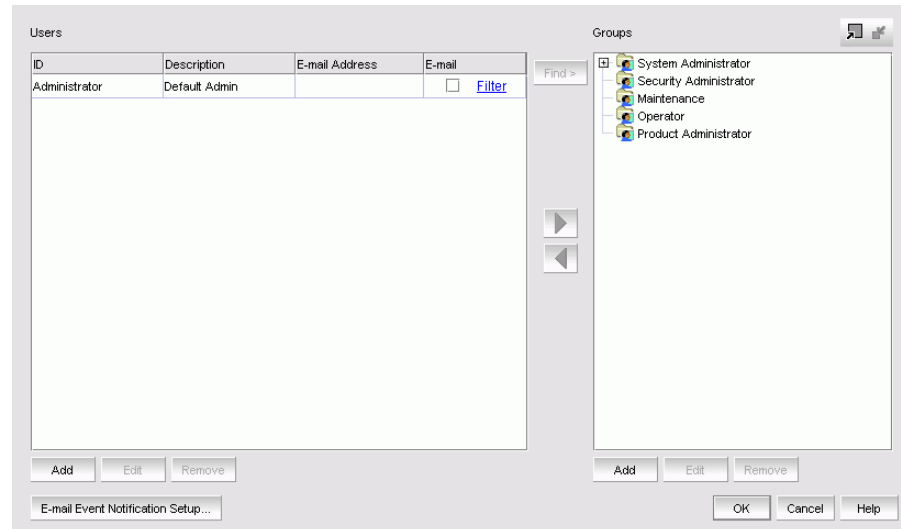
## Managing Users

When you set up users and user groups, you can add, change, or remove users. By adding a user, you assign privileges to certain features or views in the application, enhancing the security of your SAN.

### Viewing the List of Users

Select **SAN > Users**.

The **9.7 Server Users** dialog box displays users, their event notification settings, and their e-mail addresses ([Figure 12](#)).



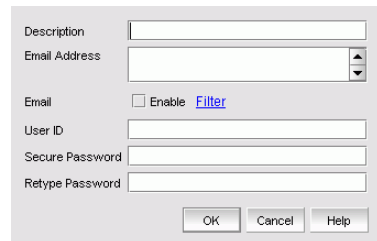
**FIGURE 12** EFCM 9.7 Server Users Dialog Box

## Adding a User Account

### NOTE

You must have the User Management privilege to perform this task.

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
2. Click **Add**.  
The **Add User** dialog box displays ([Figure 13](#)).



The screenshot shows the 'Add User' dialog box with the following fields and controls:

- Description:** A text input field.
- Email Address:** A text input field with a dropdown arrow on the right.
- Email:** A section containing an unchecked ☐ labeled 'Enable' and a blue [Filter](#) link.
- User ID:** A text input field.
- Secure Password:** A text input field.
- Retype Password:** A text input field.
- Buttons:** 'OK', 'Cancel', and 'Help' buttons at the bottom right.

**FIGURE 13** Add User Dialog Box

3. In the **Description** field, type the description of the user.
4. In the **E-mail Address** field, type the users' e-mail addresses, separating multiple addresses with a semicolon (;).
5. Select the **Enable** option to enable e-mail notification for the user.  
A message may display stating that you have enabled event notification for this user but event notification for the SAN is turned off, do you want to enable event notification for the SAN. Click **Yes**.
6. Click the **Filter** link to specify the event types for which to send e-mail notification to this user.  
For detailed instructions, refer to "[Filtering Event Notifications for a User](#)" on page 92.
7. In the **User ID** field, type a unique user name (127-character limit) for the user.
8. In the **Secure Password** and **Retype Password** fields, type the user's password (127-character limit).
9. Click **OK** to close the **Add User** dialog box.  
The new user displays on the **EFCM 9.7 Server Users** dialog box.
10. Click **OK** to save your changes and close the **EFCM 9.7 Server Users** dialog box.

## Changing a User Account

---

**NOTE**

You must have the User Management privilege to perform this task.

---

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
2. In the **Users** table, select the user whose information you want to edit.
3. Click **Edit**.  
The **Edit User** dialog box displays.
4. Edit the information as necessary.
5. Click **OK** to close the **Edit User** dialog box.  
The edited information displays on the **EFCM 9.7 Server Users** dialog box.
6. Click **OK** to save your changes and close the **EFCM 9.7 Server Users** dialog box.

## Removing a User Account

---

**NOTE**

You must have the User Management privilege to perform this task.

---

---

**ATTENTION**

You are not prompted for confirmation before the user's account is removed. If users are logged in when you remove their accounts, they receive a message that states that their client has been disconnected. They are immediately logged out after they click OK on the message.

---

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays
2. Select the user account you want to remove.
3. Click **Remove**.
4. Click **OK**.

Filtering Event Notifications for a User

The application provides notification of many different types of SAN events. If a user only wants to receive notification of certain events, you can filter the events specifically for that user.

**NOTE**  
The e-mail filter in EFCM is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

- 1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
- 2. In the **E-mail** column, click the **Filter** link associated with the user for whom you want to filter events.  
The **Define Filter** dialog box displays (Figure 14). The **Selected Events** table includes the events of which this user is notified. The **Available Events** table includes all other events.

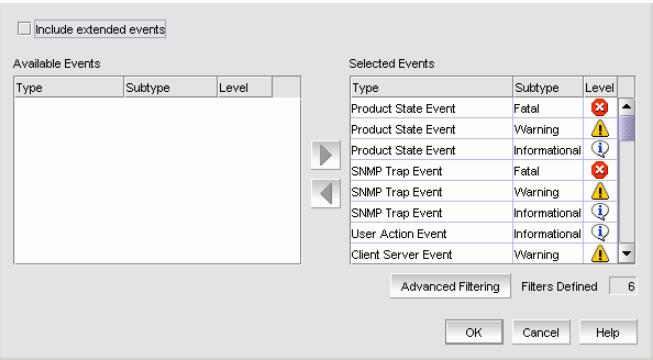


FIGURE 14 Define Filter Dialog Box

- 3. Move events between the tables by selecting the event and clicking the appropriate arrow.
- 4. To set up advanced event filtering, click **Advanced Filtering**.  
For more information about advanced event filtering, refer to “[Setting Up Advanced Event Filtering](#)” on page 93.
- 5. Click **OK**.
- 6. On the **EFCM 9.7 Server Users** dialog box, turn on event notification for the user by selecting the check box next to **Filter**.
- 7. Click **OK** to save your changes and close the **EFCM 9.7 Server Users** dialog box.

## Setting Up Advanced Event Filtering

To set up advanced event filtering on the selected events, complete the following steps.

1. Select **SAN > Users**.

The **EFCM 9.7 Server Users** dialog box displays.

2. In the **E-mail** column, click the **Filter** link associated with the user for whom you want to filter events.

The **Define Filter** dialog box displays. The **Selected Events** table includes the events of which this user is notified. The **Available Events** table includes all other events.

3. Click **Advanced Filtering**.

The **Advanced Event Filtering** dialog box displays.

4. Select the event type you want to remove from the **Event Type** drop down list.

All event types are listed in alphabetical order.

5. Enter all or part of the event type description text in the **Description Contains** text box (up to 40 characters).

This text should be the same text that displayed in the **Description** field for the events that displayed on the Master Log.

6. Click the right arrow button to move the event type to the **Additional Filters - Filter out these Events** table.

7. Click **OK**.

The **Define Filter** dialog box displays.

8. Click **OK** to close **Define Filter** dialog box.

# Managing User Groups

This section provides an overview of user groups and describes how to configure and manage user groups.

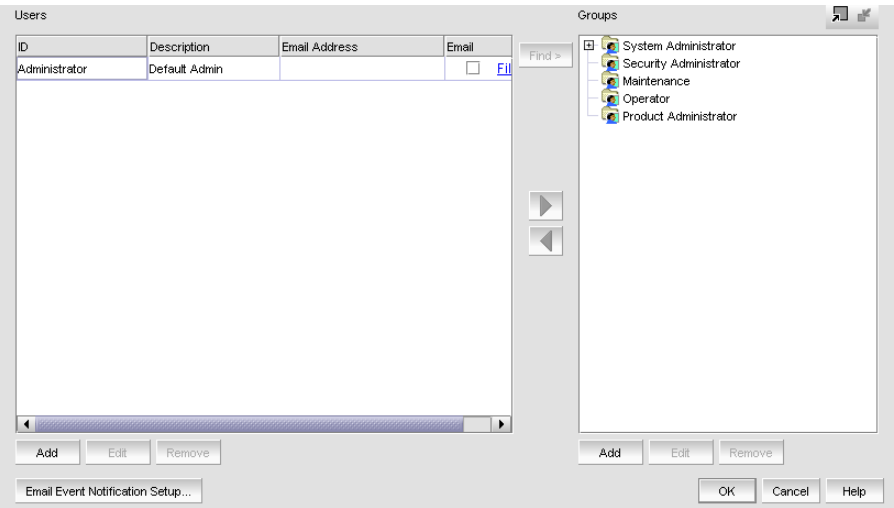
- Creating a User Group .....94
- Editing a User Group .....96
- Removing a User Group .....97
- Assigning Users to Groups .....98
- Removing a User from a Group.....99
- Finding a User’s Groups .....99

## Creating a User Group

**NOTE**  
You must be a System Administrator or Security Administrator to perform this task.

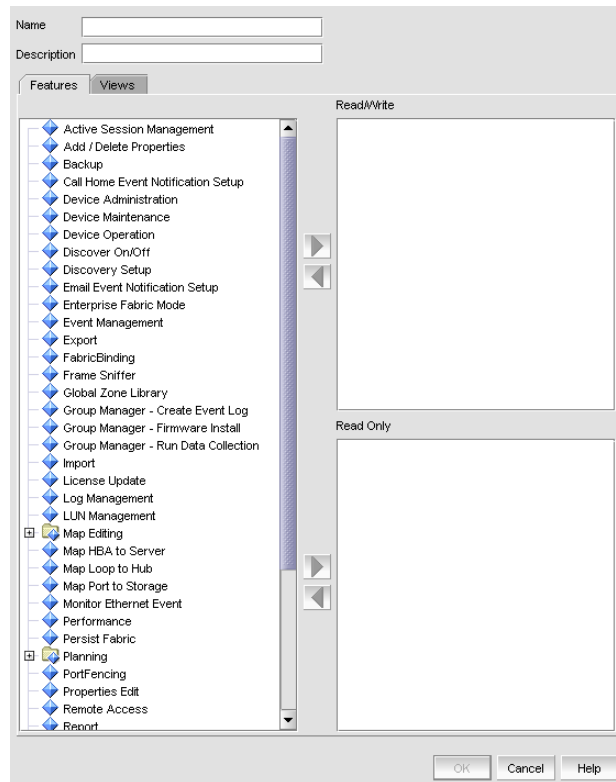
You can create a user group and specify access to certain features or views in the application, enhancing the security of your SAN.

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays (Figure 15).



**FIGURE 15** EFCM 9.7 Server Users Dialog Box

2. Click the **Add** button.  
The **Features** tab of the **Group** dialog box displays, and lists the available features (Figure 16).



**FIGURE 16** Group Features Dialog Box

3. Enter a name and description for the group in the fields provided.
4. To allow access to specific features, click the **Features** tab. Otherwise, skip to step 5.

**NOTE:** You must assign a feature to the **Read/Write** or **Read Only** list for the new group to have access to a selected feature.

- a. In the list on the left, select features to which you want to allow read and write access. Press **CTRL** and click to select multiple features.

**NOTE:** Depending on your licensed modules, the list of features may differ.

- b. Click the right arrow next to the **Read/Write** list.

The features are moved to the **Read/Write** list.

- c. In the list on the left, select features to which you want to allow read only access. Press **CTRL** and click to select multiple features.

- d. Click the right arrow next to the **Read Only** list.

The features are moved to the **Read Only** list.

5. To change permissions to use certain views, click the **Views** tab. Otherwise, skip to step 6.
  - a. In the list on the left, select views to which you want the user group to have access. Press **CTRL** and click to make multiple selections.
  - b. Click the right arrow next. The views are moved to the **Selected Views** List.

6. Click **OK** to save the new group and close the **Group** dialog box.  
The new group displays in the **Groups** list of the **EFCM 9.7 Server Users** dialog box. To add users to this group, follow the instructions in [“Assigning Users to Groups”](#) on page 98.
7. Click **OK** to save your changes and close the **EFCM 9.7 Server Users** dialog box.

### Editing a User Group

---

#### NOTE

You must have the User Management privilege to perform this task.

---

You can change a user group's permissions to use certain features and views. This provides added security for your SAN as well as your management application.

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
2. Select a user group in the **Groups** list.
3. Click **Edit** located below the **Groups** list.  
The **Group** dialog box displays.
4. To change permissions to use certain features, click the **Features** tab. Otherwise, skip to step 5.
  - a. In the **Read/Write** list, select the features to which you want to remove read and write access.  
Press **CTRL** and click to select multiple features.
  - b. Click the left arrow next to the **Read/Write** list.  
The features are moved to the list on the left.
  - c. In the **Read Only** list, select the features to which you want to remove read only access.  
Press **CTRL** and click to select multiple features.
  - d. Click the left arrow next to the **Read Only** list.  
The features are moved to the list on the left.
5. To change permissions to use certain views, click the **Views** tab. Otherwise, skip to step 6.
  - a. In the **Selected Views** list, select the views to which you want to remove access.  
Press **CTRL** and click to make multiple selections.
  - b. Click the left arrow to move the selections to the list on the left.
6. Click **OK** on the **Group** dialog box to save your edits and close the dialog box.
7. Click **OK** to save your changes and close the **EFCM 9.7 Server Users** dialog box.

## Removing a User Group

---

**NOTE**

You must have the User Management privilege to perform this task.

---

---

**ATTENTION**

You are not prompted for confirmation before the user's account is removed. If users are logged in when you remove their accounts, they are immediately logged out.

---

You can remove a user group regardless of whether a user is assigned to the group.

1. Select **SAN > Users**.

The **EFCM 9.7 Server Users** dialog box displays.

2. In the **Groups** list, select the group you want to remove.
3. Click **Remove**.
4. Click **OK** to save your changes and close the dialog box.

## Assigning Users to Groups

### NOTE

You must have the User Management privilege to perform this task.

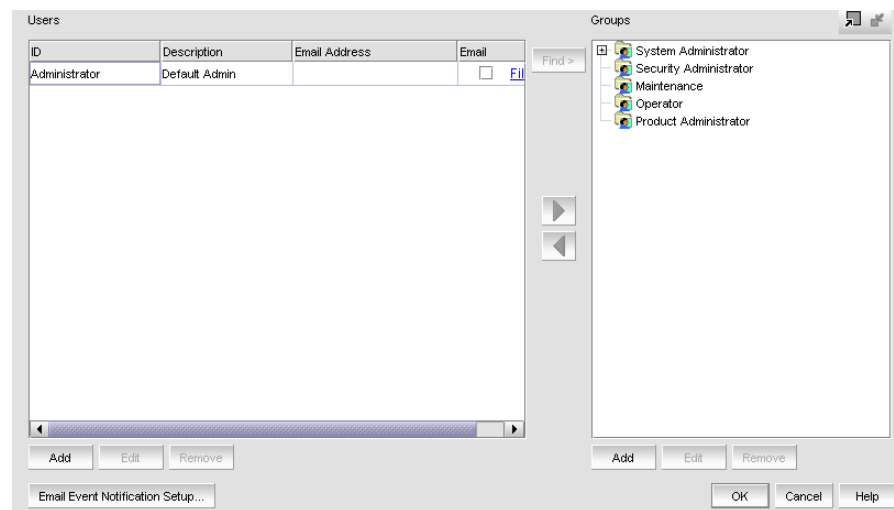
You can assign users to groups to assign them permissions for features and topology views. If you assign one user to multiple groups, the user has the user rights specified in all the groups.

### NOTE

If users are logged in when you reassign their group, they are not affected until they log out and try to log in again.

1. Select **SAN > Users**.

The **EFCM 9.7 Server Users** dialog box displays (Figure 17).



**FIGURE 17** EFCM 9.7 Server Users Dialog Box

2. In the **Users** list, select a user.
3. In the **Groups** list, select the groups to which you want to assign the user.  
Press **CTRL** and click to make multiple selections.
4. Click the right arrow.  
The user is assigned to the selected groups.
5. Click **OK**.

## Removing a User from a Group

---

**NOTE**

You must have the User Management privilege to perform this task.

---

You can remove users from groups to take away permissions for features and topology views.

---

**NOTE**

If users are logged in when you reassign their group, they are not affected until they log out and try to log in again.

---

1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
2. In the **Groups** list, select the groups from which you want to remove the user.  
Press **CTRL** and click to make multiple selections.
3. Click the left arrow.  
The user is removed from the selected groups.
4. Click **OK** to save your changes and close the dialog box.

## Finding a User's Groups

---

**NOTE**

Any user with User Management read-only or read-write privilege can find a user's group.

---

You can determine the groups to which a user belongs through the **EFCM 9.7 Server Users** dialog box.

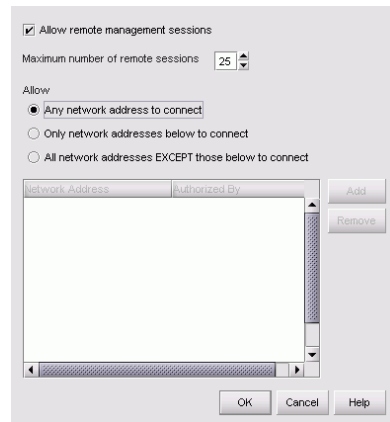
1. Select **SAN > Users**.  
The **EFCM 9.7 Server Users** dialog box displays.
2. Select a user from the **Users** list.
3. Click the **Find** button.  
The groups to which the user belongs are highlighted in the **Groups** list.
4. Click **OK** to save your changes and close the dialog box.

## Configuring Remote Access

You can specify the network addresses that can have access to the Server.

1. Select **SAN > Remote Access**.

The **Remote Access** dialog box displays (Figure 18).



**FIGURE 18** Remote Access Dialog Box

2. Select the **Allow remote management sessions** check box to allow others to access the Server remotely.
3. Enter the maximum number of remote sessions you want to allow.
4. From the **Allow** options, choose whether to allow all or some network addresses to connect.
5. (Optional) If you selected **Only network addresses below to connect** or **All network addresses EXCEPT those below to connect**, add and remove addresses in the table at the bottom of the dialog box.
  - To add an address, click **Add**, enter a network address, and click **OK**.
  - To remove an address, select the address from the table and click **Remove**.

The SAN Management application accepts IP addresses in IPv4 and IPv6 formats.

IPv4 addresses are normally written as four groups of three decimals.

IPv6 addresses are normally written as eight groups of four hexadecimal digits. The SAN Management application accepts the following IPv6 address formats:

- AAAA:0AAA:0000:AAAA:AAAA:AAAA:AAAA:AAAA (Complete address including leading zeros.)
- AAAA:AAA:0:0:AAAA:AAAA:AAAA:AAAA (Compressed format with leading zeros omitted. This is the default display.)
- AAAA:AAA::AAAA:AAAA:AAAA:AAAA (Compressed format with double colons for successive hexadecimal fields of zeros.)

6. Click **OK** to save your changes and close the dialog box.

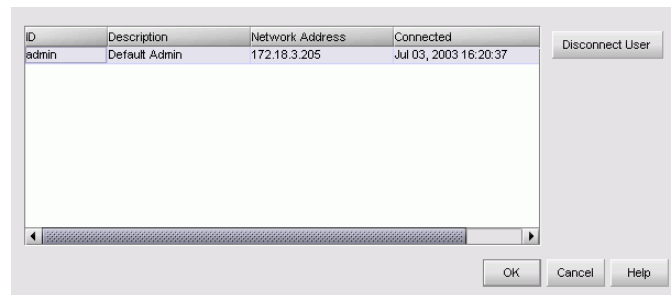
## Viewing Active User Sessions

Since more than one Client can access a Server at a time, monitoring Clients can be an important part of maintaining the SAN. View active user sessions to determine which Clients are logged into the Server.

1. Select **SAN > Active Sessions**.

The **Active Sessions** dialog box displays (Figure 19).

The **Active Sessions** dialog box lists the connected users, their network addresses, and the date and time when they logged in. If a user is logged in from more than one location, there is a separate entry for each session.



**FIGURE 19** Active Sessions Dialog Box

2. View users and the network addresses from which they connected.
3. (Optional) Select a user and click **Disconnect User** to disconnect the user from the Server.

The Server immediately shuts down the Server-Client connection. The status bar on the Client displays that the Server connection was lost. When the client is disconnected, the user sees a message and is logged out.

**NOTE:** To prevent this user from reconnecting, remove the user account through the **EFCM 9.7 Server Users** dialog box. For instructions, refer to [“Removing a User Account”](#) on page 91.

## Partitioned Switch Support

Release 9.7 displays the logical configurations of partitioned switches. Remember the following when viewing logical configurations on the topology:

- The physical set of Cisco switches display in isolated switches.
- All current view settings are used when displaying logical configurations.
- Partitioned switches are identified by their logical WWNs, not their physical WWNs.
- Cisco switch element managers provide the physical information about the switches and fabrics.
- All port information is equivalent to the physical port information.

### Viewing the Logical Configuration of Devices

You can view the logical configuration (virtual SANs) of devices on the Topology (Physical Map) and Product List.

1. Locate the virtual SAN on the topology or the Product List.
2. View switches, ISLs, and end nodes in the virtual SAN.
3. View the switch's properties using the **Properties** dialog box or the Product List.
4. View the VSAN's name and principle switch's WWN through the **Fabric Properties** dialog box.

Fibre Channel networks use World Wide Names to uniquely identify nodes and ports within nodes. For many devices, the 64-bit WWNs are fixed, and their assignment follows conventions established by the IEEE. For other devices, the WWNs may be set or modified by the user. World Wide Names are a special concern for the SAN Management application because of the following reasons:

- WWNs are used as the primary keys to identify network elements.
- Experience has been that an ill-formed WWN is evidence of a malfunctioning device.

Proper operation with the SAN Management application requires that WWNs be unique within the network and well-formed (they must be 64 bits in length and the first byte cannot be zero).

## Customizing the Main Window

You can customize the main window to display only the data you need by displaying different levels of detail on the Physical Map (topology) or Product List.

### Zooming In and Out of the Physical Map

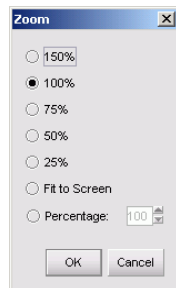
You can zoom in or out of the Physical Map to see products and ports.

#### Zooming In

To zoom in on the Physical Map, use one of the following methods:

- Click the zoom-in icon (🔍) on the toolbox.
- Press CTRL + NumPad+ on the keyboard.
- Use the **Zoom** dialog box.
  - a. Select **View > Zoom**.

The **Zoom** dialog box displays (Figure 20).



**FIGURE 20** Zoom Dialog Box

- b. Select a zoom percentage.
- c. Click **OK**.

#### Zooming Out

To zoom out of the Physical Map, use one of the following methods:

- Click the zoom-out icon (🔍) on the toolbox.
- Press or CTRL + NumPad- on the keyboard.
- Use the **Zoom** dialog box.
  - a. Select **View > Zoom**.

The **Zoom** dialog box displays.

- b. Select a zoom percentage.
- c. Click **OK**.

### Showing Levels of Detail on the Physical Map

You can view different levels of detail on the Physical Map, making SAN management easier.

#### View Fabrics

To view only fabrics, without seeing groups, products or ports:

Select **View > Show> Fabrics Only**.

#### View Groups

To view only groups and fabrics, without seeing products or ports:

Select **View > Show> Groups Only**.

#### View Products

To view products, groups, and fabrics:

Select **View > Show> All Products**.

#### View Ports

To view all ports:

Select **View > Show> All Ports**.

### Turning Flyovers On or Off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product's properties.

To turn flyovers on or off, select **Enable Flyover Display** from the **View** menu.

### Viewing Flyovers

On the Physical Map, rest the pointer over a product icon, port, or connection.

The pop-up window containing the product, port, or connection information displays.

# Customizing Device Properties

You can customize the device **Properties** dialog boxes to display only the data you need by adding, deleting, hiding, hiding all empty, or showing only property fields with data. You can also edit property fields to change the label or description of the field.

## Adding a Property Field

You can add a new field to any of the tabs from the **Properties** dialog box.

---

**NOTE**

Adding a property field is not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab to which you want to add a property.
3. Right-click on any label.  
The new property label displays above the one you select.
4. Select **Add**.  
The **Add Property** dialog box displays.
5. Type a label and description for the property.
6. From the **Type** list, select the property type, if available.
7. From the **Icon** list, select an icon to display in the column.
8. Click **OK**.  
The new property displays.

## Editing a Property Field

You can edit any fields on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to edit a property.
3. Right-click the label for the property you want to edit.
4. Select **Edit**.  
The **Edit Property** dialog box displays.
5. Change the label and description for the property, as needed.

6. From the **Type** list, change the property type, if available.
7. From the **Icon** list, select an icon to display in the column.
8. Click **OK**.

### Deleting a Property Field

You can delete any field on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to delete a property.
3. Select **Delete**.
4. Right-click the label for the property you want to delete.  
A message box displays, asking you to confirm the deletion.
5. Click **Yes**.  
The property you selected is deleted.

### Hiding a Property Field

You can hide any field on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to hide a property.
3. Right-click the label for the property you want to hide.
4. Select **Hide**.  
The property you selected is removed from the dialog box.

## Hiding All Empty Property Fields

You can hide all empty fields on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to hide a property.
3. Right-click the label for the property you want to hide.
4. Select **Hide All Empty**.

All properties without any values are removed from the dialog box.

## Showing a Property Field

You can show any field you have previously hidden on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to show a property.
3. Right-click the label above where you want the property to show.
4. Select **Show**, then select the property you want to display.  
The property you selected displays beneath the label you selected.

## Showing All Property Fields

You can show all fields you have previously hidden on any of the tabs from the **Properties** dialog box.

---

**NOTE**

Not available in the Planned SAN view.

---

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to show a property.
3. Right-click the label above where you want the properties to show.
4. Select **Show**, then select **All**.  
All properties in the **Show** list display beneath the label you selected.

### Showing Only Property Fields with Data

---

**NOTE**

Not available in the Planned SAN view.

---

You can show all fields that contain data on any of the tabs from the **Properties** dialog box.

1. Right-click any product icon and select **Properties**.  
The **Properties** dialog box displays.
2. Select the tab on which you want to show a property.
3. Right-click the label above where you want the properties to show.
4. Select **Show**, then select **Show All With Data**.

All properties in the **Show** list that contain data display beneath the label you selected.

## Export and Import

The import and export features are important functions of the application. You can import and export data for many reasons, including to communicate issues to the support center, and capture network status.

---

**NOTE**

You can export to and import from only the same releases of the application.

---

You can export files from the SAN Management application to a MySQL or an IBM® DB2® database. To set up the third-party databases, refer to the following instructions.

### Exporting Data to Disk or E-mail

The **Export Discovered SAN** dialog box displays a list of file types that can be exported, and their sizes. You can export various SAN files to a disk or e-mail.

You can also export to database, such as MySQL or DB2. For instructions for exporting to database, refer to [“Exporting Data to a Database”](#) on page 113.

1. Select **SAN > Export**.

The **Export Discovered SAN** dialog box displays a list of file types that can be exported, and their sizes ([Figure 21](#)).

Export To: **Disk** [Select All] [Unselect All]

Files	Size	Actions
<input type="checkbox"/> SAN file	15 KB	
<input type="checkbox"/> Performance data	5 KB	[Select Switch...]
<input type="checkbox"/> Master log	1 KB	[Select Events...]
<input type="checkbox"/> Connectivity map	16 KB	
<input type="checkbox"/> Connectivity XML		
<input type="checkbox"/> Product list	2 KB	
<input type="checkbox"/> Reports	0 KB	[Select Reports...]
<input type="checkbox"/> Nicknames	0 KB	
<input type="checkbox"/> Status		
<input type="checkbox"/> Zone set activation history	0 KB	
<b>Total</b>		

Export To: C:\Program Files\EFCM 9.6\Client\Data\san070925140800\ [Browse...]

[OK] [Cancel] [Apply] [Help]

**FIGURE 21** Export Discovered SAN dialog box

2. In the **Export To** list, select one of the following options:

- **Disk.** Saves the exported zip files to a user-specified directory.
- **E-mail.** Mails the exported files as an e-mail attachment.

**NOTE:** Connectivity XML cannot be exported to e-mail.

To export to both **Disk** and **E-mail** at the same time, complete steps 2 through 5 (as needed) for each option.

3. Select the types of files you want to export.

**NOTE:** Some file types may not be available based on the export destination you selected in the previous step.

Click **Select All** to select all check boxes or click **Unselect All** to clear all check boxes.

- **SAN Files.** Exports the SAN files.
  - **Performance Data.** Exports the performance data.  
Performance Monitoring is a feature of the Advanced Module, which is an Enterprise Edition only optional module. Please contact your sales representative to order the Advanced Module.
  - When exporting to Disk or E-mail, this option is subordinate to SAN Files. When exporting to MySQL or DB2 it is independent of SAN Files.
  - **Master log.** Exports the Event files.
  - **Connectivity Map.** Exports the Connectivity Map (topology) as a graphic JPG file.
  - **Connectivity XML.** Exports description of all fabric topologies in XML format, including online and persisted product and connection information.
  - Connectivity XML cannot be exported to e-mail.
  - **Product List.** Exports the Product List in tab-delimited format. To view the product list in table format, open it in Microsoft® Excel.
  - The Product List cannot be imported back into the SAN Management application.
  - **Reports.** Exports SAN reports.
  - **Nicknames.** Exports nicknames.
  - **Status.** Exports SAN status data used by technical support.
  - **Zone set activation history.** Exports the zone set activation history as an XML file. Allows you to choose the location (default is <Install\_Home>\Server\Data\Zoningsets) of where to export the zone set activation history.
4. If you are exporting to disk, skip to step 6. Otherwise, continue to step 5.

5. If you are exporting to **e-mail**, use the following fields and buttons.
  - **Mail To.** Enter the recipient's e-mail address. Separate multiple e-mail addresses with a semi colon (;).
  - **Mail List** button. Click to select from a list of e-mail addresses.
  - **From.** Enter your e-mail address.
  - **Subject.** Enter a subject for the e-mail message.
  - **Message.** Enter content for the e-mail message.
6. Click **Apply** or **OK** to export the files.
7. If you exported to disk, make a note of the file location and name. Click **OK** at the confirmation window.

## Selecting an E-Mail Address for Export

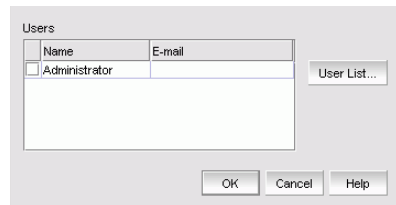
The SAN Management application enables you to select the e-mail address to which you export information.

1. Select **SAN > Export**.

The **Export Discovered SAN** dialog box displays.

2. From the **Export To** list, select **E-mail**.
3. Click **Mail List**.

The **Mail List** dialog box displays ([Figure 22](#)).



**FIGURE 22** Mail List Dialog Box

4. In the **Users** table, select a user or click **User List** to display a list of all users.
5. Click **OK**.

The selected e-mail information displays in the **Mail To** field.

## Defining Filters for Export

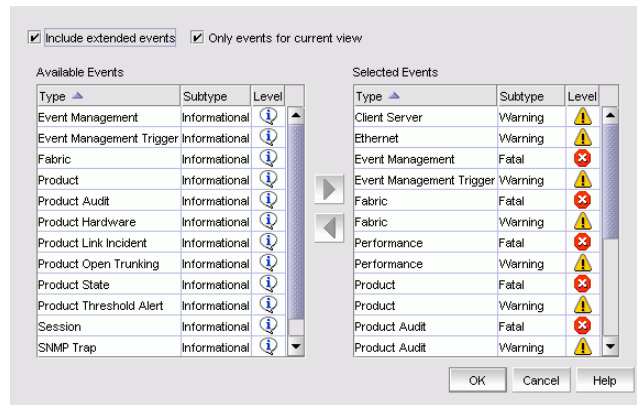
The SAN Management application enables you to filter the events included in the export of the Master Log.

1. Select **SAN > Export**.

The **Export Discovered SAN** dialog box displays.

2. Select **Master log**.
3. Click **Select Events**.

The **Define Filter** dialog box displays ([Figure 23](#)).



**FIGURE 23** Define Filter Dialog Box

4. Select the **Include extended events** check box to include extended events.
5. Select the **Only events in the current view** check box to only include events in the current view.
6. To add an event type to the filter, select the event from the **Available Events** table and click the right arrow.
7. To remove an event type from the filter, select the event from the **Selected Events** table and click the left arrow.
8. Click **OK**.

## Exporting Data to a Database

You can only export SAN files and Performance data to a third-party database, such as MySQL or DB2.

### NOTE

Export to a DB2 database is only supported on the Windows platform.

You can also export to disk or e-mail. For instructions for exporting to disk or e-mail, refer to [“Exporting Data to Disk or E-mail”](#) on page 109.

1. Configure your SAN Management application for exporting to a database.

For more information, refer to [“Setting Up for Exporting to a MySQL Database”](#) on page 115 and [“Setting Up for Exporting to a DB2 Database”](#) on page 115.

2. Select **SAN > Export**.

The **Export Discovered SAN** dialog box displays a list of file types that can be exported, and their sizes.

3. From the **Export To** list, select:

- **MySQL.** Exports data to a MySQL database. You must have a MySQL database set up to use this feature.
- **DB2.** Exports data to a DB2 database. You must have a DB2 database set up to use this feature.

4. Select the types of files you want to export.

**NOTE:** Some file types may not be available based on the export destination you selected in the previous step.

- **SAN Files.** Exports the SAN files.
- **Performance Data.** Exports the performance data. Performance Monitoring is a feature of the Advanced Module, which is an Enterprise Edition only optional module. Please contact your sales representative to order the Advanced Module.

**NOTE:** When exporting to Disk or E-mail, this option is subordinate to SAN Files. When exporting to MySQL or DB2 it is independent of SAN Files.

5. Enter information in the following fields:

- **Instance Name (DB2 only).** The DB2 instance name.
- **Host IP (MySQL only).** The IP address where the MySQL database resides. The SAN Management application accepts IP addresses in IPv4 or IPv6 formats.
- **Port (MySQL only).** The port number used to connect to the MySQL database.
- **DB Driver.** The location of the database driver.
- **User ID.** The User ID for the database.
- **Password.** The Password for the database.
- **Save Password.** To save the database password.
- **DB Name.** A name for the database export.
- **Auto generated.** To have the application generate a database name for the database export.

**NOTE:** If **Auto generated** is cleared without giving a database name, a database name is automatically created.

6. Click **Apply** or **OK** to export the files.
7. Click **OK** at the confirmation window.

## Setting Up for Exporting to a MySQL Database

You can export files from the SAN Management application to a MySQL database. Use these instructions to set up for exporting to a MySQL database.

---

**NOTE**

Your MySQL account must have a password for the export feature to work correctly.

---

1. Create a new folder on your computer.
2. Download the supported version of the JDBC driver from the MySQL website (<http://www.mysql.com/downloads/api-jdbc.html>) to the folder you created. Note the full path.

**NOTE:** You must download the appropriate driver for the MySQL server version in your environment.

3. Follow the MySQL documentation for extracting the JDBC driver into the created folder.
4. To export files to a MySQL database, follow the instructions in “[Exporting Data to a Database](#)” on page 113.

## Setting Up for Exporting to a DB2 Database

You can export files from the SAN Management application to a DB2 database. Use these instructions to set up for exporting to a DB2 database.

---

**NOTE**

Export to a DB2 database is only supported on the Windows platform.

---

1. Set up the DB2 client on the machine running the Server.

Verify that the DB2 client is in the path before the Server is started.

**TIP:** On Windows the path is C:\Program Files\sqlib\bin.

2. Create an instance on the database Server.

If the database happens to be a remote database, configure the DB2 Client to access the instance that you want to use.

The SAN Management application uses the JDBC application driver (db2java.zip) to connect to DB2.

The driver can be found in the Java folder after the DB2 Client is installed.

3. To export files to a MySQL database, follow the instructions in “[Exporting Data to a Database](#)” on page 113.

## Importing Data

You can choose to import the following information to the application:

- **SAN File (zip).** Imports an entire SAN in zip format. For step-by-step instructions about importing a SAN file, refer to [“Importing a SAN File”](#) on page 118.
- **SANvergence Manager Data.** Imports an mSAN List (created using SANvergence Manager) which contains the discovered mSAN IDs, user-defined labels, SAN Router details, and Zoning files, as well as other information. For step-by-step instructions about importing SANvergence Manager data, refer to [“Importing SANvergence Manager Data”](#) on page 119.

**NOTE:** You must exit SANvergence Manager before starting an import from the SAN Management application. SANvergence Manager only stores the contents of the discovered devices after you exit the application. Therefore, if SANvergence Manager is running during the SAN Management import, you may not receive all IP addresses from the mSAN list.

**NOTE:** SANvergence Manager has a different zone data structure than the SAN Management application; therefore, it must be converted into a data structure that can be re-used by SAN Management application. When using SAN Management application to import zones, SAN Management application only converts the data into the SAN Management application data structure and stores the data (xml files) in the `<Install_Home>` directory (`<Install_Home>\Client\Data\Zoning`) where you can access them using the **Import** button on the **Zoning** dialog box to save them into the current Zone Library. For more information, refer to the *Zoning User Manual* or Zoning Online Help.

- **Nicknames.** Imports the nicknames that were assigned using the SAN Management application and displays them on the Physical Map and Product List as product labels. Nicknames must have been defined in the **Node List View** of the SAN Management application. Nicknames defined in the **Configure Ports** area is not imported. For step-by-step instructions about importing nicknames, refer to [“Importing Nicknames”](#) on page 120.

If the WWN identifies a port or both a port and a node, the following actions occur:

- The nickname is always given to the port.
- If special handling is selected for the port's node (either HBA or Storage-Tape-Bridge) the nickname is also given to the node.

**NOTE:** The Storage-Tape-Bridge special handling selection may not work if you use LUN Management. LUN Management is an optional module available to previous LUN Management licensed customers.

- If the node has multiple ports, the nickname from the first port on the device is given to the node. If the WWN identifies a node of any kind, the nickname is always given to the node (never to the node's ports).

- **Properties (csv).** Imports properties of products and ports, including nicknames and IP addresses. The general format for this import is in comma-separated value (CSV) ASCII format. The first line defines the kind of import (Node or Port) and lists the properties and columns in the Product List. The first column must be either **Node Name** or **Port Name**. Subsequent columns contain property (column) names. These properties may be standard (for example, **Label**), or user-defined (for example, **Cabinet Color**). Non-editable properties are not imported (for example, **Port Count**). Non-existent columns are ignored. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data. To import port properties, use the **Port Name** column header. Port import only allows the **Port Nickname** property to be set. For step-by-step instructions about importing properties, refer to [“Importing Properties”](#) on page 120.

**NOTE:** You cannot import fabric type user-defined properties because both the Fabric WWN and the Switch WWN share the same WWN. When a WWN is imported using the CSV format, the WWN refers to the Switch rather than the Fabric. You can edit the user-defined properties at the Fabric Level in the SAN Management application.

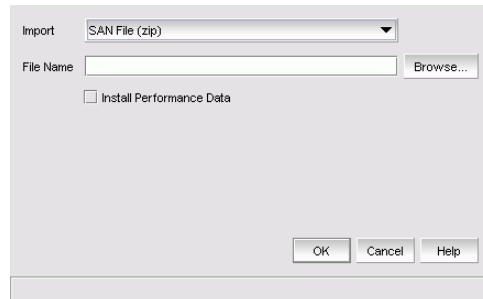
- **Server HBA Mappings (csv).** Imports Server HBA Mappings into the existing Fabric Map. The general format for this import is in CSV ASCII format. The first row contains the header for the file, which does not effect the import process; however, text must be present. The first two fields must be the WorldWideNodeName (WWNN), then the Server Nickname. If either of these fields (WWNN or Server Nickname) have no text in them, the Server HBA Mapping entry is considered null and is not imported. All additional fields are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data. For step-by-step instructions about importing Server HBA mappings, refer to [“Importing Server HBA Mappings”](#) on page 121.
- **Storage Port Mappings (csv).** Imports Storage Port Mappings into the existing Fabric Map. The general format for this import is in CSV ASCII format. The first row contains the header for the file, which does not effect the import process; however, text must be present. The first two fields must be the World Wide Port Name (WWPN), then the Storage Array Nickname. If either of these fields (WWPN or Storage Array Nickname) have no text in them, the Storage Port Mapping entry is considered null and is not imported. All additional fields are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data. For step-by-step instructions about importing storage port mappings, refer to [“Importing Storage Port Mappings”](#) on page 121.
- **Zone set activation history.** Imports zone set files in zip format. The imported Zone set activation history files are stored in <Install\_Home>\Server\Data\Zoningsets. Allows you to import the zone set activation history into another Server's zone set library, or to a different zone set library on the current server. For step-by-step instructions about importing the zone set activation history, refer to [“Importing the Zone Set Activation History”](#) on page 121.
- **FC Aliases into Nicknames.** Imports Zone Alias information from a B model switch into the SAN Management application. For step-by-step instructions about importing FC aliases into nicknames, refer to [“Importing FC Aliases into Nicknames”](#) on page 122.

## Importing a SAN File

To import a SAN File (zip), complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays (Figure 24).



**FIGURE 24** Import Dialog Box

2. Select **SAN File (zip)** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

**NOTE:** The default path is:

<Install\_Home>\ClientData\san<date>\san\*.zip. Be sure to select the san\*.zip file for import. Importing the rep\*.zip file causes errors.

**NOTE:** If you browsed to and selected the

<Install\_Home>\Server\Universe\_Home\TestUniverse\\_Working\ directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. To install performance data, click the **Install Performance Data** check box.
5. Click **OK**.

A message displays, stating that imported data will replace corresponding data on the server. The client is logged out and the **EFCM 9.7 Log In** dialog box displays. Log back into the application.

---

### ATTENTION

When discovery is on, the discovered SAN is replaced with the imported data. Only one SAN can be viewed at a time. For instructions about turning on discovery, refer to [“Setting Up Discovery”](#) on page 139.

---

6. On the **Imported Results** dialog box, click **OK**.

## Importing SANvergence Manager Data

EFCM 9.7 allows you to import your SANvergence Manager data. The SANvergence Manager data includes discovery information (mSAN and SAN Router details), user-defined labels, SNMP traps, TFTP paths, and Zoning files, as well as other information.

---

### NOTE

You must exit SANvergence Manager before starting an import from the SAN Management application. SANvergence Manager only stores the contents of the discovered devices after you exit the application. Therefore, if SANvergence Manager is running during the SAN Management import, you may not receive all IP addresses from the mSAN list.

---

---

### NOTE

SANvergence Manager has a different zone data structure than the SAN Management application; therefore, it must be converted into a data structure that can be re-used by the SAN Management application. When importing SANvergence Manager zones, the SAN Management application only converts the data into the SAN Management application data structure and stores the data files (xml files) in the <Install\_Home> directory (<Install\_Home>\Client\Data\Zoning). You can then access them using the Import function on the Zoning dialog box to save them into the current Zone Library. For more information, refer to the *Zoning User Manual* or Zoning Online Help.

---

To import SANvergence Manager Data files, complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. From the **Import** list, select **SANvergence Manager Data**.
3. In the **Installation Path** field, enter the path to the SANvergence Manager directory or **Browse** to the directory.

The default path is: C:\Program Files\McDATA\SANvergence Manager 4.7.

4. Click **OK**.

When the import is complete and successful, a User Action Event entry is created in the Master Log.

### Importing Nicknames

To import Nicknames, complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **Nicknames** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

**NOTE:** If you browsed to and selected the `<Install_Home>\Server\Universe_Home\TestUniverse\_Working\` directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. Select one of the following options to set special handling for nicknames assigned to ports:

- For HBA ports, also apply the nickname to the HBA product.
- For Storage ports, apply one of the nicknames to the Storage product. (Storage ports include the product types Storage, Tape, and Bridge.)

**NOTE:** This is only applicable when nicknames have been set to allow non-unique nicknames in the **Options** dialog box. For more information, refer to [Configuring Nickname Settings](#).

5. Click **OK**.

A Warning message displays stating “*Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname. Do you want to continue?*”. Click **OK** to continue.

6. On the **Imported Results** dialog box, click **OK**.

### Importing Properties

To import Properties (csv), complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **Properties (csv)** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

**NOTE:** If you browsed to and selected the `<Install_Home>\Server\Universe_Home\TestUniverse\_Working\` directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. Click **OK**.

Importing properties replaces corresponding data on the server. Any data actively being monitored by the SAN Management application will revert to the discovered values.

5. On the **Imported Results** dialog box, click **OK**.

## Importing Server HBA Mappings

To import Server HBA Mappings (csv), complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **Server HBA Mappings (csv)** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

**NOTE:** If you browsed to and selected the <Install\_Home>\Server\Universe\_Home\TestUniverse\\_Working\ directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. Click **OK**.
5. On the **Imported Results** dialog box, click **OK**.

## Importing Storage Port Mappings

To import a Storage Port Mappings (csv), complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **Storage Port Mappings (csv)** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

**NOTE:** If you browsed to and selected the <Install\_Home>\Server\Universe\_Home\TestUniverse\\_Working\ directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. On the **Imported Results** dialog box, click **OK**.

## Importing the Zone Set Activation History

To import Zone set activation history (zip), complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **Zone set activation history (zip)** from the **Import** list.
3. In the **File Name** field, enter the path and file name or **Browse** to the file.

The imported Zone set activation history files are stored in <Install\_Home>\Server\Data\Zoningsets.

**NOTE:** If you browsed to and selected the <Install\_Home>\Server\Universe\_Home\TestUniverse\\_Working\ directory or any files within that directory, the Import/Export might fail. You must deselect the file or directory before you run the Import/Export process again.

4. Click **OK**.

The zone set you want to import is compared to zone sets in the destination zone library. If no zone name or zone ID conflicts are found, the zone set is successfully imported and the **Import** dialog box closes.

However, note the following exceptions:

- If the destination library contains a zone set that is identical to the one being imported, a message displays asking whether you want to proceed. Click **Yes** to continue and overwrite the existing zone set with the one being imported, or click **No** to cancel the import operation.
- If the destination library contains a zone set with the same name as the one being imported but different contents, a message displays warning you that continuing will overwrite the existing zone set, and asking whether you want to proceed. Click **Yes** to overwrite the existing zone set, or click **No** to cancel the import operation.

### Importing FC Aliases into Nicknames

To import Zone Alias information from a B model switch into the SAN Management application., complete the following steps.

1. Select **SAN > Import**.

The **Import** dialog box displays.

2. Select **FC Aliases into Nicknames** from the **Import** list.

3. In the **Fabric** field, select the fabric from which you want to import FC Aliases.

4. Click **OK**.

A Warning message displays stating “*Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname. Do you want to continue?*”. Click **OK** to continue.

The file is imported and assigned.

# Accessing Third-Party Tools

You can add third-party tools to the **Tools** menu or shortcut menus to open other software products you frequently use.

## Adding a Tool

You can specify third-party tools so they appear on the **Setup Tools** dialog box. From there, you can add them to the **Tools** menu and then open the tools directly from the management application.

- 1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

- 2. Click the **Tools Menu** tab.
- 3. Click **Define**.

The **Define Tools** dialog box displays (Figure 25).

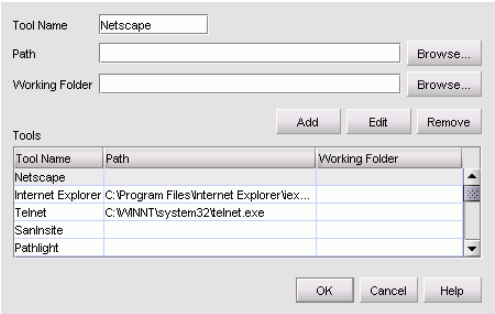


FIGURE 25 Define Tools Dialog Box

- 4. In the **Tool Name** field, type the tool’s name as you want it to appear on the **Setup Tools** dialog box.
- 5. In the **Path** field, type or browse to the path of the executable file.
- 6. In the **Working Folder** field, type or browse to the path of the folder that you want to set as your working folder.
- 7. To add the tool, click **Add**.

The **Setup Tools** dialog box displays with the new tool added to the **Tools Menu Item** table.

**NOTE:** You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

- 8. Click **OK** to save your work and close the **Setup Tools** dialog box.

### Removing a Tool

You can remove a tool from the third-party tool list.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.
3. Click **Define**.

The **Define Tools** dialog box displays.

4. In the **Tools** table, select the row of the tool you want to remove.
5. Click **Remove**.

If the tool is not being utilized, no confirmation message displays.

**NOTE:** You must click **Remove** before clicking **OK**; otherwise, your changes will be lost.

6. Click **OK** to save your work and close the **Setup Tools** dialog box.

### Adding an Option to the Tools Menu

You can add options to the **Tools** menu to launch tools directly from the application.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. In the **Menu Text** field, type a label for the option as you want it to appear on the **Tools** menu.
4. Select the application from the **Tool** list, or click **Define** if you want to specify a new tool.

For instructions, refer to [“Adding a Tool”](#) on page 123.

5. (Optional) In the **Parameters** field, enter parameters, such as a URL.
6. (Optional) In the **Keystroke** list, select a keyboard shortcut.
7. Click **Add**.

The new tool displays in the **Tool Menu Items** table.

**NOTE:** You must click **Add** before clicking **OK**; otherwise, the new menu option is not created.

8. Click **OK** to save your work and close the **Setup Tools** dialog box.

The tool you configured now displays on the **Tools** menu.

## Changing an Option on the Tools Menu

You can edit parameters for third-party tools that display on the **Tools** menu.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

The **Tool Menu Items** table displays all configured tools, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. In the **Tool Menu Items** table, select the tool you want to edit.

The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the fields as desired.

5. Click **Edit**.

**NOTE:** You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

6. If you changed the name of a tool, you are prompted to verify the change. Accept the change.
7. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Removing an Option from the Tools Menu

You can remove an option listed on the **Tools** menu.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

3. Select the tool you want to remove from the **Tool Menu Items** table.

The settings for the selected tool displays in the fields at the top of the dialog box.

4. Click **Remove**.

**NOTE:** You must click **Remove** before clicking **OK**; otherwise, your changes will be lost.

5. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Adding an Option to a Device's Shortcut Menu

You can add an option to a device's shortcut menu.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

The **Product Popup Menu Items** table displays all configured shortcut menu options.

3. In the **Menu Text** list, type or select the text as you want it to appear on the menu.

4. Select **Match Conditions** or **All**.

- Select **Match Conditions** to display the menu option only for devices that meet the conditions listed.

- Select **All** to display the menu option on the shortcut menus for all devices.

If you selected **All**, skip to step 7. Otherwise, continue to step 5.

5. Select a **Property** name and **Value** for Condition 1.

6. (Optional) To define a second condition to be simultaneously true, enter the **Property** name and **Value** for Condition 2 (Condition 1 AND Condition 2 must be true).

**NOTE:** To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

7. From the **Tool** list, select the tool that you want to launch, or click **Define** to add a tool.

For more information, refer to [“Adding a Tool”](#) on page 123.

8. Click **Append device ID** to specify the parameter used when opening the tool.

- Select **IP Address** to specify that the device's IP address should be used when opening the tool.

- Select **Node WWN** to specify that the device's Node WWN should be used when opening the tool.

9. Click **Add** to add the new menu item.

It displays in the **Product Popup Menu Items** table.

**NOTE:** You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

10. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Changing an Option on a Device's Shortcut Menu

You can change the parameters for a tool that displays on a device's shortcut menu.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

The **Product Popup Menu Items** table displays all configured shortcut menu options.

3. In the **Product Popup Menu Items** table, select the menu item you want to change.

The settings for the selected menu item displays in the fields at the top of the dialog box.

4. Edit the fields, as necessary.

5. Click **Edit**.

**NOTE:** You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

6. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Removing an Option from a Device's Shortcut Menu

You can remove a tool that displays on a device's shortcut menu.

1. Select **Tools > Setup**.

The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

The **Product Popup Menu Items** table displays all configured menu options.

3. In the **Product Popup Menu Items** table, select the menu item you want to remove.

4. Click **Remove**.

**NOTE:** You must click **Remove** before clicking **OK**; otherwise, your changes will be lost.

5. Click **OK** to save your work and close the **Setup Tools** dialog box.

## Launching a Telnet Session

You can use Telnet to log in and issue command line-based commands to a switch.

1. On the Physical Map, select the switch to which you want to connect.

**NOTE:** The switch must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the **Tools** menu or the shortcut menu. You must right-click the device icon, select **Properties**, and enter the device's IP address before you can open a Telnet session.

2. Select **Tools > Product Menu > Telnet**.

The Telnet session window displays.

**NOTE:** On Linux systems, you must use CTRL + BACKSPACE to delete text in the Telnet session window.

### Launching an Element Manager

Element Managers are used to manage Brocade Fibre Channel switches and directors. You can open a device's Element Manager directly from the application.

On the Physical Map, right-click the Brocade device you want to manage and select **Element Manager**.

The Element Manager displays.

### Blade Switch Element Manager Requirements

The following requirements must be met to allow a Blade Switch Element Manager to be launched from EFCM.

- The firmware must be EOS/q 5.2.2 or greater.
- The "Switch Licensed for EFCM capability" feature must be enabled on the Blade Switch.
- The WWN must be set to "080088" in the Vendor ID field on the **Features** dialog box in the Blade Switch Element Manager.

The following SNMP Sys OIDs are not configurable on the Blade Switch but can be configured within EFCM. These are the default SNMP Sys OIDs which allow the Blade Switch to be identified as a Blade Switch:

1.3.6.1.4.1.1663.1.1.1.1.21 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.29 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.37 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.38 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.39 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.40 = Brocade

1.3.6.1.4.1.1663.1.1.1.1.41 = Brocade

### Launching Web Tools

Use Brocade Web Tools to enable and manage Brocade Access Gateway, Switches, and Directors. You can open Web Tools directly from the application. For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide*. For more information about Brocade Access Gateway, Switches, and Directors, refer to the documentation for the specific device.

On the Physical Map, right-click the B model device you want to manage and select **Element Manager**.

---

#### NOTE

You must have Device Administration privileges for the selected device to launch Web Tools. If you do not have Device Administration privileges, you will need to enter those credentials to launch Web Tools.

---

Web Tools displays.

## Launching FCR Configuration

Use FCR Configuration to launch the FC Routing module, which enables you to share devices between fabrics without merging the fabrics. You can open the FC Routing module directly from the SAN Management application. For more information about FC Routing, refer to the *Brocade Fabric Manager Administrator's Guide* or *Brocade Web Tools Administrator's Guide*.

The FCR Configuration option is available only for the following devices with FOS level 5.0 or higher:

- Brocade 7500 switch
- Brocade director's configured with an FR4-18i blade

On the Physical Map, right-click the Brocade device you want to configure and select **FCR Configuration**.

The FC Routing module displays.

## Starting Third-Party Tools from the Application

You can open third-party tools from the **Tools** menu or a device's shortcut menu. Remember that you cannot open a tool that is not installed on your computer. You must install the tool on your computer and add the tool to the **Tools** menu or device's shortcut menu.

To open an application, perform the following steps.

1. Select the device.
2. Use either of the following techniques:
  - Select **Tools > Product Menu > available tool**.
  - Right-click the device, and select the tool from the menu.

## Accessing Eclipse Management Applications

Use the following procedures to access the Eclipse SAN Router management applications from your SAN Management application.

If SANvergence Manager or SAN Router Element Manager do not appear in the menu, refer to [“Adding a Tool”](#) on page 123.

- SANvergence Manager - Right-click the SAN Router icon on the Physical Map and select **SANvergence Manager** from the menu.
- SAN Router Element Manager - Right-click the SAN Router icon on the Physical Map and select **Element Manager** from the menu.

You can also launch a SAN Router Element Manager from SANvergence Manager is operating by:

- Select the SAN Router in an expanded mSAN list on the left pane of the **SANvergence Manager** window, then click the **Element Manager** icon at the top of the **SANvergence Manager** window.
- Select the SAN Router in the **SAN Routers** table in the right pane of the **SANvergence Manager** window when an mSAN cloud is selected, then click the **Element Manager** icon at the top of the **SANvergence Manager** window.

---

### NOTE

You cannot launch SANvergence Manager or Element Managers by selecting the router proxy port icons (domain IDs 30 and 31). You must select the icon for the actual SAN Router.

---

For details on using SANvergence Manager to manage Eclipse SAN Routers in your SAN, refer to the *SANvergence Manager User Manual*.

For details on using Element Manager applications to configure specific SAN Routers, refer to the following publications:

- *Eclipse 1620 SAN Router Administration and Configuration Manual*.
- *Eclipse 3300/4300 SAN Routers Administration and Configuration Manual*.
- *Eclipse 2640 SAN Router Administration and Configuration Manual*.

# Discovering a SAN

---

## In this Chapter

The SAN Management application discovers products, fabrics, and connections in a SAN. Through this powerful tool, you can manage and monitor your SAN in real-time, ensuring that any issues are resolved immediately. This chapter provides instructions for configuring the discovery feature.

- How Discovery Works .....132
- Manager of Manager Discovery .....134
- Setting Up Discovery .....139
- Setting the Polling Delay .....141
- Configuring Address Properties .....142
- Turning Discovery On and Off .....151
- Determining the Discovery State .....151
- Troubleshooting Discovery .....152
- Configuring Storage Port Mapping .....155

## How Discovery Works

Discovery is the process by which the application contacts the devices in your SAN. When you log in to a Server, the local network is automatically discovered and displayed on the Physical Map. When you configure and turn on discovery, the application discovers products connected to the SAN. The application illustrates each product and its connections on the Physical Map (topology). For details, refer to “[Setting Up Discovery](#)” on page 139.

The SAN Management application enables you to discover devices using Out-of-Band and In-Band discovery. For detailed information, refer to “[Out-of-Band Discovery](#)” on page 132 and “[In-Band Discovery](#)” on page 132.

### Out-of-Band Discovery

When performing out-of-band discovery, the application connects to the switches through the IP network and product information is copied from the SNS database on the switch to the Server.

To correctly discover all SAN products, you must specify each product's IP address or a subnet on the **Out-of-Band** tab of the **Discover Setup** dialog box. If you do not configure the application to directly discover the devices, the connections and attached devices may not display correctly. Only fabrics that have manageable switches as the principal switch display. For a list of manageable products, refer to [Table 22 Product Icons](#) on page 243. If a manageable switch is being directly managed, but exists in a fabric where the principal switch is a third-party device, another Server is not allowed to connect to and manage those devices.

---

**NOTE**

Only one copy of the application should be used to monitor and manage the same devices in a subnet.

---

### In-Band Discovery

When performing in-band discovery, the Server gathers data from the HBA driver about the in-band data flow and LUNs. Discovery is performed by calling SCSI commands from the vendor's library and sending them through the HBA to the target LUNs on the storage device.

Note that for in-band discovery to work properly, the HBA driver must support the Fibre Alliance HBA API. Furthermore, the vendor's HBA drivers and their implementation of the SNIA HBA API Library must be correct. With the HBA vendor's drivers and library installed, the application is able to gather information about both the adapter's and the port's attributes.

When in-band discovery starts, the application calls routines from the vendor's library and the library issues SCSI Inquiry, Report LUNs, and Read Capacity commands through Fibre Channel. When the devices respond, the libraries deliver information about the discovered ports back to the application.

For information about supported HBA driver levels, please go to the <http://www.brocade.com/support/resources> website and follow the instructions to access the *Compatibility Matrix*.

# DataFabric Manager Interaction Requirements

## Gathering DataFabric Manager Device Discovery Data

You must configure SAN Manager to gather device discovery data directly from DataFabric Manager. For more information, see [“Configuring the Product Type and Access”](#) on page 149.

## SNMP Trap Listener Conflict

DataFabric Manager also listens for SNMP traps on UDP port 162. If you install the SAN Manager server and DataFabric Manager on the same machine, you must do the following to avoid a port conflict with the DataFabric Manager SNMP trap listener:

1. Specify a port other than 162 in the SNMP Trap Listener Port option (banner > Options link > SNMP Trap Listener Options) in DataFabric Manager.
2. Configure SAN Manager to forward traps to the SNMP trap listener on the port that you specified in Step 1. For more information about configuring SNMP trap forwarding, see [“Configuring Trap Forwarding”](#) on page 197.

## Manager of Manager Discovery

### NOTE

Servers running SANavigator cannot be discovered.

EFCM (9.0 and higher) provides a Manager of Managers (MoM) feature that enables you to discover data from other servers (target servers) in the SAN and manage EFCM switches through the discovered target servers. The discovering server (MoM server) can be used to communicate and access multiple versions of EFCM, view performance across fabrics, and perform select management actions such as zoning. This allows you to create a consolidated “single pane” view across multiple fabrics and locations managed by multiple EFCM server instances.

Once the MoM server discovers the target server, it obtains the basic discovery information through SNMP, such as the target server description and sysObjectID. The rest of the basic discovery information is from the EFCM switches currently being managed by the target server. The management of the target server and its attached switches is through ECC-API discovery. The following table details the features which are available for this mode of discovery. For the sake of simplicity the server being discovered is referred to as the target server and the server discovering other servers is referred to as MoM server.

Management of the Manager of Manager requires that any of the following ports must be accessible to allow EFCM to EFCM communications: 51511, 51513, 52688, 53865, 55042, 56219, 57396, 58573, or 1099.

The following table is applicable only to the switches discovered by the target server. Switches directly managed by the MoM server, have all the capabilities.

**TABLE 18** Manager of Manager ECC-API Discovery

MoM Server	Target Server
<p>Only MPI managed switches (see below) display in the topology with the generic icon.</p> <ul style="list-style-type: none"> <li>• Brocade M4700F Switch</li> <li>• Brocade M-6140 Director</li> <li>• Brocade M-i10K Director</li> <li>• ED-5000 Director</li> <li>• Sphereon 3016 Switch</li> <li>• Sphereon 3032 Switch</li> <li>• Sphereon 3216 Switch</li> <li>• Sphereon 3232 Switch</li> <li>• Sphereon 4400 Switch</li> <li>• Sphereon 4500 Switch</li> <li>• Sphereon 4710 Switch</li> <li>• Intrepid 6064 Director</li> </ul> <p>All switches connected to the managed switches display with the generic icons.</p> <p>Devices display as unmanaged switches (gray).</p> <p>The MoM server displays a consolidated view of the discovered servers.</p>	<p>All managed switches display in the topology with the specific icons.</p> <p>All switches connected to the managed switches display with the generic icons.</p>
Call Home is not available.	Call home is available.
Element Manager cannot be launched for devices discovered through a target server.	Element Manager can be launched.
Enterprise Fabric Mode is not available.	Enterprise Fabric Mode is available.

**TABLE 18** Manager of Manager ECC-API Discovery

MoM Server	Target Server
Events are not passed back to the MoM server.	Events are available.
Fabric Binding is not available.	Fabric Binding is available.
Firmware code loads are not available.	Firmware code loads are available.
Nicknames are not available.	Nicknames are available.
Performance information displays in the topology (for example, marching ants, real time performance graphs, and historical performance graphs).	Performance information displays in the topology (for example, marching ants, real time performance graphs, and historical performance graphs).
Port Fencing is not available.	Port Fencing is available.
Security Center is not available.	Security Center is available.
Show Route supported for the managed switches.	No Show Route support for the switches discovered via the target server.
Virtual Fabrics are discovered and displayed but cannot be configured from the MoM server.	Virtual Fabrics is available.
Zoning is available. Zoning Scope and Zoning Library contains selections for all discovered fabrics as well as the discovered target servers.	Zoning is available. Zoning Scope and Zoning Library contains selections for all discovered fabrics.
For all other features the MoM server has the same level of support as the Target server.	

## Discovering Data From Another EFCM Server

To discover another server and manage a SAN with remote sites, complete the following steps.

1. Select **Discover > Setup**.

The **Discovery Setup** dialog box displays.

2. Click the **Out-of-Band** tab.
3. Click **Add**.

The **Address Properties** dialog box displays.

4. Specify the IP addresses you want to discover.
  - a. On the **IP Address** tab, enter a description for the device at the new IP address.
  - b. Select **IPv4 Address** or **IPv6 Address**.
    - If you selected **IPv4 Address**, enter the IP address and subnet mask for the device.
    - If you selected **IPv6 Address**, enter the IP address and prefix length for the device.
  - c. In the **Data Source for Domain** area, select the **Use auto detection** option.

- d. (Optional) To generate a sequence of IP addresses, complete the following steps.

**NOTE:** You can only generate a sequence of IP addresses using the IPv4 format.

- 1) In the **Add Multiple** area, click **Generate a sequence of IP addresses**.

This eliminates the need to add each IP address individually.

- 2) In the **Last IP** field, enter the last IP address in the sequence.

All IP addresses in a sequence must be on the same subnet and have the same first three octets.

5. Click the **SNMP** tab and edit the default settings, if needed.

To change the SNMP default settings, refer to [“Configuring an SNMP Community String”](#) on page 147.

6. Click the **Product Type and Access** tab.

- a. From the **Product Type** list, select **EFCM Server**.

- b. In the **User ID** field, enter a user ID.

**NOTE:** Make sure your User ID has Administration rights to the EFCM Server you discover.

- c. In the **Password** and **Retype Password** fields, enter the password.

7. Click **OK** on the **Address Properties** dialog box.

8. Repeat steps 1 through 8 for each device that you want to discover.

9. From the **Available Addresses** table, select the IP address you want to add to discovery.

10. Click the right arrow button next to the **Selected Individual Address** table.

The selected addresses display in the **Selected Individual Address** table.

11. Click **OK** on the **Discover Setup** dialog box.

The selected devices display in the EFCM main window, indicated by the Server icon.

## License Discovery

License discovery is only available with the EFCM 9.7 server. If you discover a EFCM 7.X or 8.X server, their licenses will not affect the MoM server license.

When configured correctly, the MoM server obtains the license key and serial number from the target server and then updates its license information with any target server licensed port count and additional modules. To configure the MoM server to obtain license information, refer to [“Generating an Aggregate Advanced Module Licensed Port Count”](#) on page 137.

The MoM server license updates every time a target server is added or removed from the active discovery list. However, the state of the target server (offline/online) does not affect the license. Note that when the MoM server detects a change in the licensed port count or modules, it forces the clients connected to the MoM server to logout (same behavior as license updates).

## Generating an Aggregate Advanced Module Licensed Port Count

To discover the license keys from managed EFCM servers and update the Manager of Manager (MoM) server license, complete the following steps.

1. Select **Help > License**.

The **License** dialog box displays.

2. Select the **Aggregate advanced module licensed port counts from all managed EFCM servers** check box.
3. Click **OK**.

A message displays, warning you that you have changed the aggregate port count setting, click **Yes** to continue.

After the next discovery cycle, the MoM server updates the licensed port count and modules list to include information from all discovered managed EFCM servers. Clients connected to the MoM server are logged out automatically and must log in again.

## Mi10K Director Discovery

Management of the Mi10K Director utilizes various network protocols to gather and send data. Complete and successful management of the Mi10K Director requires that all the ports associated with the network protocols must be accessible through the network and unblocked by any firewalls.

- Simple Management Network Protocol (SNMP) across a User Datagram Protocol (UDP) connection (primary) which uses the default network port 1024.
- Transmission Control Protocol / Internet Protocol (TCP/IP) connection (additional) which uses two protocols across the TCP/IP connection.
  - Extensible Markup Language - Remote Procedure Call (XML-RPC) uses port 80.
  - NMRU, Brocade proprietary protocol, uses port 2048 for non-SSL and port 2049 for SSL connections.

---

### NOTE

Make sure that your SNMP communication parameters are set correctly to discover Brocade or IBM switches. Otherwise, the discovery may fail.

---

## Access Gateway Discovery

---

### NOTE

Only supported on B model and M model switches that support NPIV functionality.

---

EFCM 9.5 (and higher) supports discovery of Brocade Access Gateway. Brocade Access Gateway is a feature of the Brocade Fabric OS (5.2.1 or higher) and a mode of operation designed for Brocade blade server SAN switches. Access Gateway uses N\_Port ID Virtualization (NPIV) standards to connect server blades to any SAN fabric. Access Gateway does not appear as switch to the fabric, it does not add a domain or require the same level of management as a traditional switch.

If discovered directly without discovering connected switches, Access Gateway displays in an isolated devices group with the generic icon; however, no connected devices display. Access Gateway is manageable through Web Tools (right-click device and select **Element Manager**).

If discovered directly with direct discovery of connected switches, Access Gateway displays in an isolated device group with the generic icon and all connected end devices display as a collapsed host group connected to an edge switch in the Topology Map and as NPIV devices beneath the real edge switch port (to which Access Gateway is physically connected) in the Product List.

If discovered indirectly (discover the edge switch to which Access Gateway is physically connected), Access Gateway does not display in the Topology Map. All connected end devices display as an collapsed NPIV host group connected to an edge switch in the Topology Map.

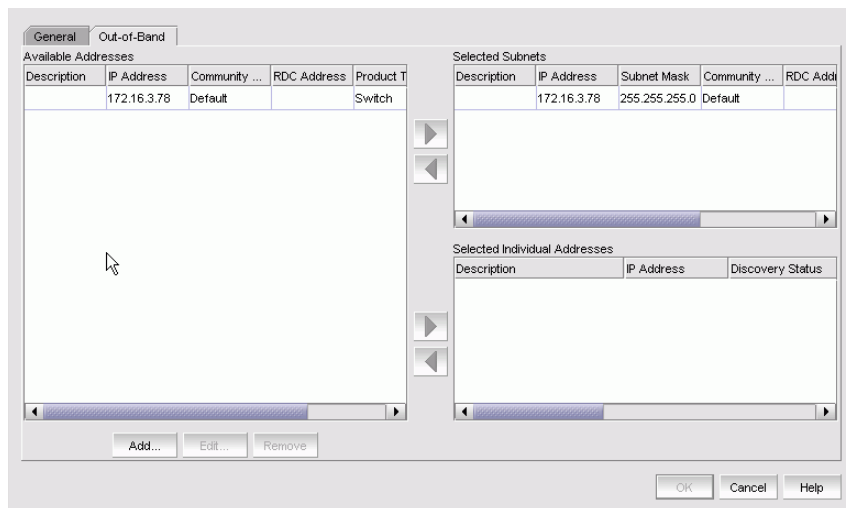
For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide*. For more information about Brocade Access Gateway, refer to the *Brocade Access Gateway Administrator's Guide*.



4. Select the discovery method you want to use.
    - Select the **Out-of-Band Discovery Enable** check box to perform out-of-band discovery. Continue with step 8.  
For more information, refer to “[Out-of-Band Discovery](#)” on page 132.
    - Select the **In-Band Discovery Enable** check box to perform in-band discovery. Go to step 5.  
For more information, refer to “[In-Band Discovery](#)” on page 132.

**NOTE:** To perform in-band discovery, an HBA must be physically installed in the Server. Download the vendor’s HBA drivers and libraries from the vendor’s website.

  - Select both options to perform both in-band and out-of-band discovery. Continue with step 5.
5. If you selected **In-Band Discovery**, in the **Available HBAs** table, select the **Active** check box for each HBA you want to use to discover the SAN.
  6. Select **Clear current SAN devices before starting new discovery** to start discovery with a clean desktop.
  7. Select the **Rebuild Discovery Schedule** check box to reset the discovery engine and rebuild the discovery catalog.
    - If you selected **Out-of-Band Discovery**, continue with step 8.
    - If you only selected **In-Band Discovery**, go to step 12.
  8. Click the **Out-of-Band** tab ([Figure 27](#)).



**FIGURE 27** Discover Setup Dialog Box (Out-of-Band Tab)

9. Specify the IP addresses you want to discover through out-of-band discovery.

**NOTE:** If you change the password on the Switch or Director, you must enter the new password during discovery on the Product Type and Access tab of the Address Properties dialog box.

### ATTENTION

To correctly discover all SAN products, you must specify each product’s IP address or a subnet in the **Discover Setup** dialog box’s **Out-of-Band** tab. If you do not configure the application to discover the devices directly, the connections and attached devices may not display correctly.

10. Select IP addresses from the **Available Addresses** table and click the right arrow to add them to the **Selected Subnets** or **Selected Individual Addresses** tables.
11. Click **Add** to specify the IP addresses you want to discover through out-of-band discovery.

**NOTE:** The SAN Management application cannot discover, manage, or monitor any devices when the device's Operating System has IPv6 mode.

You can add, edit, and remove IP addresses as necessary. For instructions, refer to [“Configuring Address Properties”](#) on page 142.

12. Click **OK**.
13. Select **Discover > On**.

## Setting the Polling Delay

The polling delay allows you to configure a delay between polling cycles.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click the **General** tab.
3. Edit the values in the **Polling Delay** field.

**NOTE:** To make sure performance data is accurate, set the polling delay below two minutes. If you set the polling delay to greater than two minutes, it may produce inaccurate performance data.

4. Click **OK** on the **Discover Setup** dialog box.

## Configuring Address Properties

You can configure IP Addresses, SNMP Community Strings, and Product Type and Access. Using these properties, the application can perform discovery and communication functions as well as set password authentication.

### Adding an IP Address

You can add IP addresses and subnets through which the SAN can be discovered.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click the **Out-of-Band** tab.
3. Click **Add**.

The **Address Properties** dialog box displays (Figure 28).

**NOTE:** The dialog box may display more fields or tabs depending on your licensed features.

**FIGURE 28** Address Properties Dialog Box (IP Address Tab)

4. On the **IP Address** tab, enter a description for the product at the new IP address.
5. Select either **IPv4 Address** or **IPv6 Address**.

**NOTE:** The SAN Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

6. If you selected **IPv4 Address**, complete the following steps.
  - a. In the **IPv4 Address** field, enter the IP address (four groups of three decimals) for the device.
  - b. In the **Subnet Mask** (IPv4 or dual mode only) field, enter the subnet mask address for the device.
7. If you selected **IPv6 Address**, complete the following steps.

**NOTE:** If IPV6 is disabled, restart the SAN Management server and edit the IPV6 address to IPV4 format.

  - a. In the **IPv6 Address** field, enter the address (eight groups of four hexadecimal digits) for the device.
  - b. In the **Prefix Length** (IPv6 or dual mode only) field, enter the prefix length for the device.
8. Choose from one of the following options:
  - Select the **Enable** check box, if necessary, to allow extended discovery support for a manageable M model device.

Extended discovery allows the SAN Management application to discover all devices in the same fabric as the specified device.
  - Clear the **Enable** check box to disable extended discovery support.
9. Select the data source for the domain.
  - Use auto detection
  - Use the server
  - Use a specific RDC
10. If you selected **Use a specific RDC**, enter the IP address (IPv4 format only) of the RDC in the **IP address of RDC** field.
11. (Optional) You can generate a sequence of IP addresses, which eliminates the need to add each IP address individually. To do so, complete the following steps.

**NOTE:** You can only generate a sequence of IP addresses using the IPv4 format.

  - a. In the **Add Multiple** field, click the **Generate a sequence of IP addresses** option.
  - b. In the **Last IP** field, enter the last IP address in the sequence.

All IP addresses in a sequence must be on the same subnet and have the same first three octets.
12. Click **OK** on the **Address Properties** dialog box.
13. Move the IP address to the **Selected Individual Addresses** area.
14. Click **OK** on the **Discover Setup** dialog box.

### Editing an IP Address

You can edit IP addresses or associated subnets that are listed on the **Discover Setup** dialog box.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click the **Out-of-Band** tab.
3. In the **Available Addresses** table, select the IP address to edit.
4. Click **Edit**.

If the IP address you want to edit is in the **Selected Individual Addresses** area of the **Discovery Setup** dialog box, then an message displays telling you that you must remove the IP Address from the **Selected Individual Addresses** area before editing. Click **OK** to close the message.

To remove the IP address from the **Selected Individual Addresses** area, select the IP address and click the left arrow.

5. In the **Description** field, modify the description for the device.
6. Select either **IPv4 Address** or **IPv6 Address**.

**NOTE:** The SAN Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

7. If you selected **IPv4 Address**, complete the following steps.
  - a. In the **IPv4 Address** field, enter the IP address (four groups of three decimals) for the device.
  - b. In the **Subnet Mask** (IPv4 or dual mode only) field, enter the subnet mask address for the device.
8. If you selected **IPv6 Address**, complete the following steps.
  - a. In the **IPv6 Address** field, enter the address (eight groups of four hexadecimal digits) for the device.
  - b. In the **Prefix Length** (IPv6 or dual mode only) field, enter the prefix length for the device.
9. Choose from one of the following options:
  - Select the **Enable** check box to allow extended discovery support for a manageable M model device.  
Extended discovery allows the SAN Management application to discover all devices in the same fabric as the specified device.
  - Clear the **Enable** check box to disable extended discovery support.
10. Select the data source for the domain.
  - Use auto detection
  - Use the server
  - Use a specific RDC
11. If you selected **Use a specific RDC**, enter the IP address (IPv4 format only) of the RDC in the **IP address of RDC** field.

12. Click **OK** on the **Address Properties** dialog box.
13. Move the IP address to the **Selected Individual Addresses** area.
14. Click **OK** on the **Discover Setup** dialog box.

## Enabling Extended Discovery

When you enable extended discovery for a manageable M model device, the SAN Management application discovers all devices in the same fabric as the specified device.

---

### NOTE

Extended discovery is not supported on B model devices.

---

---

### NOTE

Enabling or disabling extended discovery for any IP address causes discovery to reload.

---

To enable extended discovery, complete the following steps.

1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
2. Select the IP address you want to edit from the **Available Addresses** area and click **Edit**.  
If the IP address you want to edit is in the **Selected Individual Addresses** area of the **Discovery Setup** dialog box, then an message displays telling you that you must remove the IP Address from the **Selected Individual Addresses** area before editing. Click **OK** to close the message.  
Remove the IP address from the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, then repeat this step to edit the IP address.  
**NOTE:** You can also enable extended discovery when you are adding an IP address. For more information, refer to [“Adding an IP Address”](#) on page 142.
3. Select the **Enable** check box to allow extended discovery support for a device.  
The SAN Management application discovers all devices in the same fabric as the discovered device.
4. Click **OK** on the **Address Properties** dialog box.
5. Move the IP address to the **Selected Individual Addresses** area.
6. Click **OK** on the **Discover Setup** dialog box.

## Disabling Extended Discovery

When you disable extended discovery support for a device, the SAN Management application only discovers the devices connected to the specified device. Extended discovery is enabled by default. You should disable extended discovery if the following conditions exist:

- The fabric is an edge fabric routed through a B model router.
- The event log contains bogus events, which you want to eliminate, and the SAN Management server is managing all of the device in the fabric.

---

**NOTE**

Enabling or disabling extended discovery for any IP address causes discovery to reload.

---

To disable extended discovery, complete the following steps.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Select the IP address you want to edit from the **Available Addresses** area and click **Edit**.

If the IP address you want to edit is in the **Selected Individual Addresses** area of the **Discovery Setup** dialog box, then an message displays telling you that you must remove the IP Address from the **Selected Individual Addresses** area before editing. Click **OK** to close the message.

Remove the IP address from the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, then repeat this step to edit the IP address.

**NOTE:** You can also disable extended discovery when you are adding an IP address. For more information, refer to [“Adding an IP Address”](#) on page 142.

3. Clear the **Enable** check box.
4. Click **OK** on the **Address Properties** dialog box.
5. Move the IP address to the **Selected Individual Addresses** area.
6. Click **OK** on the **Discover Setup** dialog box.

## Removing an IP Address

You can remove IP addresses from the **Discover Setup** dialog box.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click the **Out-of-Band** tab.
3. From the **Available Addresses** table, select the IP address you want to remove.

---

### ATTENTION

When you click **Remove**, the IP address is removed without confirmation.

---

4. Click **Remove**.

If the IP address you want to edit is in the **Selected Individual Addresses** area of the **Discovery Setup** dialog box, then a message displays telling you that you must remove the IP Address from the **Selected Individual Addresses** area before editing. Click **OK** to close the message.

Remove the IP Address from the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, then repeat step 4 to remove the IP Address.

5. Click **OK** to close the **Discover Setup** dialog box.

## Configuring an SNMP Community String

You can specify the SNMP community strings used to communicate with products.

1. Select **Discover > Setup**.

The **Discover Setup** dialog box displays.

2. Click the **Out-of-Band** tab.
3. Click **Add**.

The **Address Properties** dialog box displays.

4. Click the **SNMP** tab (Figure 29).

**FIGURE 29** Address Properties Dialog Box (SNMP tab)

## 4 Configuring Address Properties

5. In the **Target Port** field, enter the target port.
6. In the **Time-out (sec)** field, enter the duration (in seconds) after which the application times out.
7. In the **Retries** field, enter the number of times to retry the process.
8. From the **SNMP Version** drop down list, select the SNMP version.
  - If you selected v1 or v2c, continue with step 9.
  - If you select v3, the SNMP tab displays the v3 required parameters. Go to step 14.
9. At the **Read** option, select **Default 'public'** or **Custom**.
10. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
11. At the **Write** option, select **Default 'private'** or **Custom**.
12. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.  
Go to step 22.
13. If you are configuring a Mi10K director, select the **Configure for Intrepid 10K** check box.
  - If you selected **Configure for Intrepid 10K**, go to step 16.
  - If you did not select **Configure for Intrepid 10K**, continue with step 14.
14. In the **User Name** field, enter a user name.

The screenshot shows the 'SNMP' tab of the 'Address Properties' dialog box. The 'IP Address' tab is also visible. The 'Product Type and Access' tab is selected. The 'SNMP' tab contains the following fields and controls:

- Target Port:** 161
- Time-out (sec):** 5
- Retries:** 2
- SNMP Version:** v3 (dropdown menu)
- Presets:** ☐ Configure for Intrepid 10K
- User Name:** (text field)
- Context Name:** (text field)
- Auth Protocol:** - None - (dropdown menu)
- Auth Password:** (text field)
- Retype Password:** (text field)
- Priv Protocol:** - None - (dropdown menu)
- Priv Password:** (text field)
- Retype Password:** (text field)

At the bottom of the dialog box are three buttons: OK, Cancel, and Help.

**FIGURE 30** Address Properties Dialog Box (SNMP Tab - v3)

15. In the **Context Name** field, enter a context name.
16. In the **Auth Protocol** field, select the authorization protocol.
17. In the **Auth Password** field, enter the authorization password.
18. In the **Retype Password** field, re-enter the authorization password.
  - If you selected **Configure for Intrepid 10K**, go to step 22.
  - If you did not select **Configure for Intrepid 10K**, continue with step 19.
19. In the **Priv Protocol** field, select the privacy protocol.
20. In the **Priv Password** field, enter the privacy password.
21. In the **Retype Password** field, re-enter the privacy password.

22. Click **OK** on the **Address Properties** dialog box.
23. Click **OK** on the **Discover Setup** dialog box.

## Reverting to a Default SNMP Community String

1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
2. Click the **Out-of-Band** tab.
3. Select an IP address from the **Available Addresses** table.
4. Click **Edit**.  
The **Address Properties** dialog box displays.
5. Click the **SNMP** tab.
6. Click **Default 'public'** and **Default 'private.'**
7. Click **OK** on the **Address Properties** dialog box.
8. Click **OK** on the **Discover Setup** dialog box.

## Configuring the Product Type and Access

You can specify the product type and set a user name and password for the address.

---

**NOTE**

The **Product Type and Access** tab may not be available in all situations.

---

1. Select **Discover > Setup**.  
The **Discover Setup** dialog box displays.
2. Click the **Out-of-Band** tab.
3. Click **Add**.  
The **Address Properties** dialog box displays.
4. On the **Address Properties** dialog box, click the **Product Type and Access** tab ([Figure 31](#)).

## 4 Configuring Address Properties



**FIGURE 31** Address Properties Dialog Box (Product Type and Access Tab)

5. Select the type of device from the **Product Type** list.
  - If you selected **<not specified>** from the **Product Type** list, go to step 8.
  - If you selected **Switch** from the **Product Type** list, go to step 6.
  - If you selected **IBM ESS Storage** from the **Product Type** list, go to step 6.
  - If you selected **HDS** from the **Product Type** list, go to step 6.
  - If you selected **Clariion** from the **Product Type** list, go to step 8.
  - If you selected **CIM/WBEM Services** from the **Product Type** list, enter a name in the **Name Space** field, and go to step 6.
  - If you selected **Symmetrix** from the **Device Type** list, go to step 8.
  - If you select **NetApp DFM** from the **Product Type** list, from the **Protocol** list, select the product protocol. In the **DFM Port** field, enter the product DFM port number. Then go to step 6.
  - If you select **HP XP Storage** from the **Product Type** list, continue with step 6.
6. In the **User ID** field, enter a user ID.
7. In the **Password** and **Retype Password** fields, enter the password.

**NOTE:** If you change the password on the Switch or Director, you must enter the new password during discovery on the **Product Type and Access** tab of the **Address Properties** dialog box.
8. Click **OK**.
9. Select the DataFabric Manager server you just added and move it to the **Selected Individual Address** list.

**NOTE:** After the initial discovery of NetApp DFM servers, the Master Log generates "Created" events for each LUN in the filers.
10. Click **OK**.

## Turning Discovery On and Off

To turn discovery on, select **Discover > On**.

To turn discovery off, select **Discover > Off**.

## Determining the Discovery State

---

**NOTE**

The Product List panel may be hidden by default. To view all panels, select **View > All Panels**, or press **F12**.

---

You can determine the discovery status of products by looking at the **Operational Status** column in the Product List. Additionally, the operational status “Unknown” is equivalent to the discovery state “Offline.” The operational statuses, “Healthy/Operational,” “Degraded/Marginal,” and “Down/Failed,” are equivalent to a discovery state of “Online.”

You can also determine the discovery status of products from the **Discover Setup** dialog box (**General Tab**) by looking at the **Discovery Status** column in the **Selected Individual Address** table.

# Troubleshooting Discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

- 1. Verify IP connectivity by pinging the switch.
  - a. Open the command prompt.
  - b. From the Server, type `ping <switch IP address>`.
- 2. Verify the SNMP settings.
  - a. Launch SANPilot or EFCM Basic by opening a web browser application and entering the IP address of the product as the Internet uniform resource locator (URL).

**NOTE:** SANPilot or EFCM Basic is only available for M model devices with M-EOS.

For example, `http://10.1.1.11`.

  - b. Log in and click **OK**.
  - c. Select **Configure > SNMP**.

The **Configure > SNMP** view displays (Figure 32).

Name	Write Auth	Trap Recipient	UDP Port
public	<input checked="" type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		
	<input type="checkbox"/>		

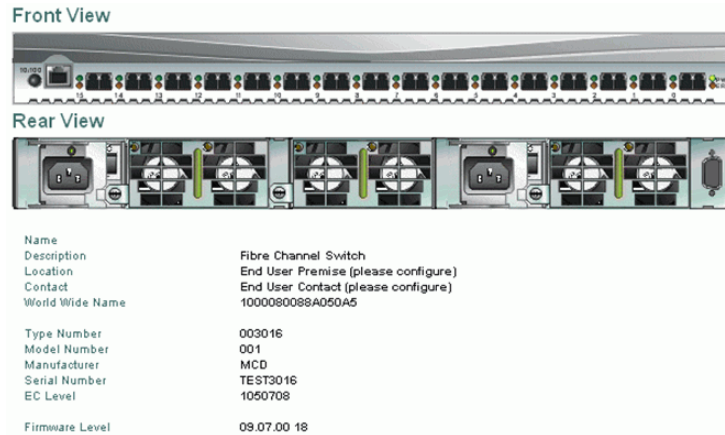
**FIGURE 32**    SNMP Settings in SANPilot or EFCM Basic

- d. Verify that the SNMP Agent is enabled.
- e. Verify that the **Name** field displays “public” or matches the SAN Management application configuration.

3. Verify the product data.

a. Select **Product > Hardware**.

The **Product > Hardware** view displays product properties.



**FIGURE 33** Product Type in SANPilot or EFCM Basic

b. Verify that the **Type Number** is one of the following.

003016  
 003032  
 003216  
 003232  
 004300  
 004500  
 005000  
 006064  
 006140

c. Verify that the **World Wide Name** has the correct syntax (xx:xx:xx:xx:xx:xx:xx).

4. Verify SNMP connectivity.
  - a. Use a third-party MIB browser to verify the SNMP connection.
  - b. Change the SNMP default timeout.
    - 1) Stop the Server.
    - 2) Increase the default SNMP settings.

If the device is running heavy traffic or is known to have slow SNMP response time, moderately increase the SNMP timeout (default time-out is one second) and retry count (default count is one retry).

These two values are controlled by two VMParameters residing in the bin\EFCMService.ini file when the application is running as a Windows service: `smp.snmp.timeout` and `smp.snmp.retries`. For example, specifying “-D`smp.snmp.timeout=5`” and “-D`smp.snmp.retries=1`” instructs the server to use five seconds as the SNMP time-out and one retry as the retry count.

**NOTE:** The higher the values, the longer discovery spends waiting for an SNMP response. This translates into slower system performance.

- 3) Restart the server.

## Configuring Storage Port Mapping

The SAN Management application enables you to see multiple ports on your storage devices in a SAN. It also displays the relationship between multiple ports and represents them as attached to a storage array (device) in the **Device Tree**, **Topology**, and **Fabric** views. Occasionally, there are cases where the SAN Management application cannot see the relationship between ports attached to the same storage device. Therefore, the SAN Management application allows you to manually associate the connections that the system is unable to make using the **Storage Port Mapping** dialog box.

The SAN Management application allows you to create and assign properties to a Storage Device during the mapping process using the **Storage Port Mapping** dialog box. Once a Storage Device has multiple ports assigned to it you cannot change the device type.

---

### NOTE

When you open the **Storage Port Mapping** dialog box, Discovery is automatically turned off. When you close the **Storage Port Mapping** dialog box, Discovery automatically restarts.

---

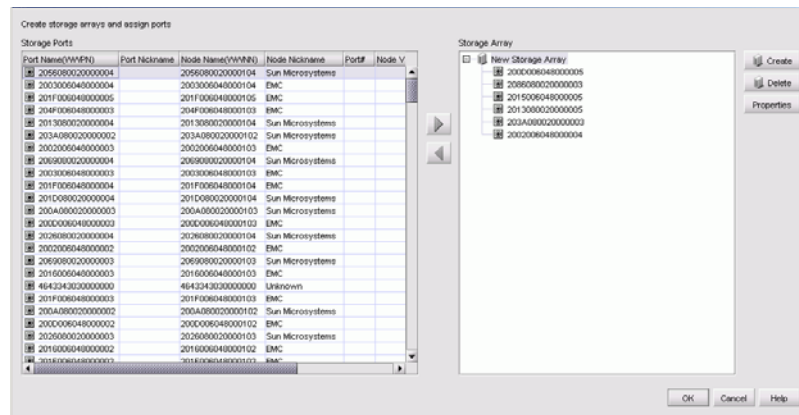
During Discovery, if a previously mapped Storage Port is found to have a relationship with a port just discovered, the SAN Management application automatically reassigns the Storage Port to the proper mapping. The two Ports are grouped together. This grouping is visually represented as a Storage Device. This Storage Device contains Node information from the discovered port and populates default information where available.

The SAN Management application allows you to change the Device Type of a discovered device. Isolated Storage Ports are represented as Storage Devices. Using the Storage Port Mapping dialog you cannot change the device type to an HBA, JBOD, and so on. However, once a device has been identified as type Storage with ports assigned, you can no longer change its type.

## Adding Storage Ports to a Storage Array

- To open the **Storage Port Mapping** dialog box, choose from one of the following steps.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box (Figure 34) displays.



**FIGURE 34** Storage Port Mapping Dialog Box

- Select a storage port from the **Storage Ports** table.
 

To select more than one port, hold down the **CTRL** key while selecting multiple storage ports.

A storage array in the **Storage Array** list is highlighted.
- Click the right arrow.
 

The selected storage port is added to the Storage Array.
- Click OK.

## Removing Storage Port and Storage Array Associations

- To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.
- Select a storage port from the **Storage Array** list and click the left arrow button.
 

The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
- Click **OK**.

## Reassigning Mapped Storage Ports

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.The **Storage Port Mapping** dialog box displays.
2. Select a storage port from the **Storage Array** list and click the left arrow button.  
The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
3. Make sure that the storage port you want to reassign is still selected.
4. Select the storage array to which you want to reassign the storage port and click the right arrow button.  
The storage port moves from the **Storage Ports** table to the selected storage array.
5. Click **OK**.

## Creating a Storage Array

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.The **Storage Port Mapping** dialog box displays.
2. Click **Create**.  
A new storage array displays in the **Storage Array** list.
3. Double-click on the new array to rename the new storage array and press **Enter**.
4. Add storage ports to the new storage array.  
For step-by-step instructions about adding port to an array, refer to [“Adding Storage Ports to a Storage Array”](#) on page 156.  
**NOTE:** You must add storage ports to the new storage array to save the new array in the system.
5. Click **OK**.

### Editing Storage Array Properties

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select the storage array in the **Storage Array** list and click **Properties**.

The **Properties** dialog box appears.

3. In the **Nickname** field, edit the storage array nickname, if necessary.
4. In the **Name** field, enter the storage array name.
5. In the **Node WWN** field, enter the storage array node WWN.
6. In the **Name (in-band)** field, enter the storage array in-band name.
7. In the **Port Count** field, enter the storage array port count.
8. In the **Port Count (in-band)** field, enter the storage array in-band port count.
9. In the **Enclosure** field, enter an enclosure for the storage array.
10. In the **IP Address** field, enter the IP address for the storage array.
11. In the **Vendor** field, enter the vendor name for the storage array.
12. In the **Vendor (in-band)** field, enter the vendor name for the in-band storage array.
13. In the **Vendor ID (in-band)** field, enter the vendor ID for the in-band storage array.
14. In the **Model #** field, enter a model number for the storage array.
15. In the **Model (in-band)** field, enter a model number for the in-band storage array.
16. In the **Serial #** field, enter a serial number for the storage array.
17. In the **Serial (in-band)** field, enter a serial number for the in-band storage array.
18. In the **Firmware** field, enter the firmware for the storage array.
19. In the **Firmware (in-band)** field, enter the firmware for the in-band storage array.
20. In the **Operational Status** field, enter a status for the storage array.
21. In the **Management Link** field, enter a management link for the storage array.
22. In the **Location** field, enter a location for the storage array.
23. In the **Contact** field, enter a contact name for the storage array.
24. In the **Description** field, enter a description for the storage array.
25. In the **Comments** field, enter any comments.
26. Click **OK** on the **Properties** dialog box to save the storage array properties.
27. Click **OK** on the **Storage Port Mapping** dialog box.

## Deleting a Storage Array

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select a Storage Array icon in the **Storage Array** list.
3. Click **Delete**.

The selected Storage Array and all Storage Ports assigned to the array are removed from **Storage Array** list. All Storage Ports assigned to the device are moved to the **Storage Ports** table.

4. Click **OK**.

## Viewing Storage Port Properties

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select a storage port from the **Storage Array** list.
3. Click **Properties**.

The **Properties** dialog box displays.

4. Review the properties.
5. Click **OK** on the **Properties** dialog box.
6. Click **OK** on the **Storage Port Mapping** dialog box.

### Viewing Storage Array Properties

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
  - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
  - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
  - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.

The **Storage Port Mapping** dialog box displays.

2. Select a storage array from the **Storage Array** list.
3. Click **Properties**.

The **Properties** dialog box displays.
4. Review the properties.
5. Click **OK** on the **Properties** dialog box.
6. Click **OK** on the **Storage Port Mapping** dialog box.

# Configuring SAN Products and Fabrics

---

## In this Chapter

This chapter provides instructions for configuring and managing products and fabrics, set threshold limits on the number of specific port events, send SNMP trap reports to other computers, count frames passed by a switch port, and configure SNMP trap agent.

- Managing Products .....162
- Configuring Nicknames.....167
- Configuring Enterprise Fabric Mode.....174
- Configuring Fabric Binding .....176
- Port Fencing.....182
- Persisting and Unpersisting Fabrics and Switch Groups .....194
- Configuring Trap Forwarding.....197
- Configuring Frame Sniffer.....199
- Configuring the SNMP Agent .....207

## Managing Products

You can use the application to manage discovered products. You can search for a product, change its properties, and perform other configuration and maintenance tasks.

### Determining Whether a Product is Being Managed

Managed devices are managed through MPI and allow you to perform numerous SAN management functions (such as, management through an Element Manager, zoning, fabric binding, enterprise fabric mode, and show route). A managed product's icon displays as a Brocade icon as shown in the Icon Legend (see ["Icon Legend"](#) on page 243). Blade Switches only allow management through a web-based Element Manager and zoning. An unmanaged product's icon displays as a generic icon or a grayed-out icon and you cannot perform any of the above mentioned SAN management functions.

To obtain management capability on a device, you need to add the device's IP address to your discovery setup (see ["Adding an IP Address"](#) on page 142).

If the device is still not manageable, check the following:

- Make sure the device is not managed by another EFCM instance.
- Make sure you have the NMRU connection (**Properties** dialog box, **Discovery Status** and/or **Managed By** fields).
- Make sure the device's state is operational (**Properties** dialog box, **Operational Status**).

Devices discovered through the Manager of Manager (MoM) feature (ECCAPI), which enables you to discover data from other servers in the fabric, allows you to access and use the Element Manager of the attached switches, view performance across fabrics, and perform select management actions such as zoning.

### Opening a Product's Element Manager

You can open an Element Manager to administer manageable switches and directors directly from the application. For a list of manageable products, refer to [Table 22 Product Icons](#) on page 243.

### Opening the Element Manager from the Interface

To open an Element Manager from the user interface, perform one of the following steps:

- On the Physical Map or Product List, right-click a manageable product's icon and select **Element Manager** or **Element Management (HTML)**.
- On the Physical Map, double-click a manageable product's icon.

**NOTE:** When you open the Element Manager for the Sphereon 4300 Fabric Switch, the EFCM Basic application also opens.

**NOTE:** If you encounter problems, ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application should be used to monitor and manage the same devices in a subnet.

## Searching for Products in a SAN

You can search a discovered SAN for a specific product by its properties, such as name or IP address.

1. Enter the search parameter in the **Search** box on the toolbar ([Figure 35](#)).



**FIGURE 35** Search Box

2. Click the up or down arrow to search forwards or backwards through the Physical Map.
3. Click **Search** to find each product.

---

### NOTE

When the application finds a product on the Physical Map, it highlights the product on the Physical Map as well as on the Product List.

---

## Changing Product Properties

You can change some of the properties for online products.

---

### NOTE

If the product you selected is offline, you will not be able to edit this information.

---

---

### NOTE

This process does not change the configuration of the product. It only changes the information that is stored on the local Server.










---


1. On the Physical Map, right-click a product icon and select **Properties** from the menu.  
The product's **Properties** dialog box displays.
2. Click the **Properties** tab.
3. Edit information as necessary.
4. When finished, click **OK** to update the product's properties on the local Server.

## Determining a Product's Operational Status

You can determine a product's operational status by looking at the Physical Map or the Product List. Both the Physical Map and the Product List enable you to determine a product's operational status by looking at the associated icons ([Table 19](#)).

**TABLE 19** Product Status Icons

Icon	Status
No icon	Healthy/Operational
	Attention
	Degraded/Marginal
	Device Added
	Device Removed/Missing
	Down/Failed
	Routed In
	Routed Out
	Unknown/Link Down
	Virtual Switch

To see a list of all products requiring attention, click the Attention Indicator icon () on the Status bar at the bottom of the main window. The **Service Request** dialog box displays with a list of the names and IP addresses of devices needing attention. Click a product name hyperlink to jump to the product on the Physical Map. The list updates dynamically.

## Showing Routes Between Two End-Products

### NOTE

This feature is only available for fabrics consisting solely of manageable M model products (refer to [Table 22 Product Icons](#) on page 243).

You can use the Show Route feature to view the path that Fibre Channel frames must take between two end-products in a multiswitch fabric. If you intend to show a different route within the same fabric, the previous route is automatically hidden.

### Requirements

To view the route between two products, the following conditions must be met:

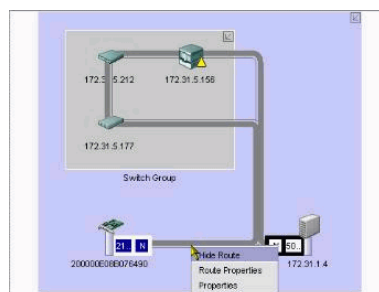
- There must be two or more switches in the fabric.
- All switches or directors in the route must be managed by the application and attached to the same Server.
- All switches or directors in the route must be manageable products and must be running firmware version M-EOS 4.0 or higher. For a list of manageable products, refer to [Table 22 Product Icons](#) on page 243.
- All attached products in the route must be in the same zone.

### Procedure

To show the route for two specific ports on the end nodes, perform the following steps:

1. In the Product List, click the + next to a switch product icon to see the nodes.
2. Right-click a node and select **Show Route**.  
The **Show Route** dialog box displays.
3. Select a destination node from the **Destination Port** table.
4. Click **OK**.

The route between the nodes displays on topology ([Figure 36](#)).



**FIGURE 36** Show Route Example

## Hiding Routes Between Two End-Products

---

**NOTE**

This feature is only available for fabrics consisting solely of manageable products (refer to [Table 22 Product Icons](#) on page 243).

---

You can use the Hide Route feature to hide routes that Fibre Channel frames must take between two end-products in a multiswitch fabric. You must show routes before you can hide routes. For instructions, refer to “[Showing Routes Between Two End-Products](#)” on page 165.

To hide the route, right-click the route (line between end-nodes), or the fabric that includes the route you want to hide and select **Hide Route**.

## Viewing Properties of Routes Between Two End-Products

1. To view the properties of a route, right-click the route and select **Properties**.  
The **Route Properties** dialog box displays.
2. Review the source and destination ports, as well as route details.
3. Click **Close** to close the dialog box.

## Changing a Fabric's Properties

You can view and change a fabric's properties.

1. On the Physical Map, right-click a fabric icon or the background of an expanded fabric and select **Properties** from the menu.

The **Fabric Properties** dialog box displays.

2. View the fabric's information and edit the nickname, if desired.

**NOTE:** If you segment a fabric, the Fabric's nickname follows the assigned principal switch.

3. Click **OK** to update the fabric's properties.

## Configuring Nicknames

The SAN Management application allows you to use Nicknames as a method of providing familiar simple names to products and ports in their SAN. Using your SAN Management application you can:

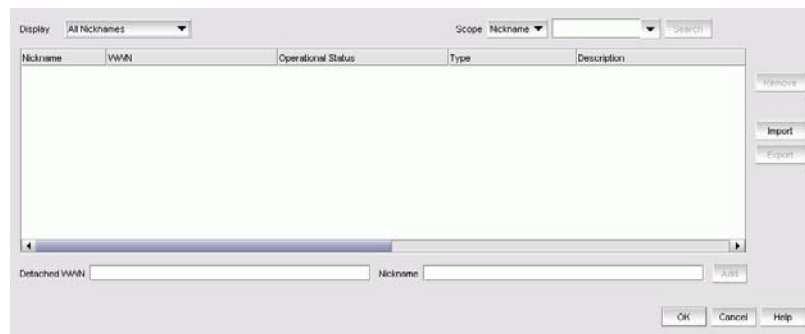
- Associate a nickname with a product or port WWN currently being discovered.
- Add a WWN and an associated nickname for a product or port that is not yet being discovered.
- Remove or disassociate a nickname from a WWN.

## Viewing Nicknames

The SAN Management application allows you to view devices by the device nickname.

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays (Figure 37).



**FIGURE 37** Configure Nicknames Dialog Box

2. From the **Display** list, select **All Nicknames**.

Only devices with a nickname display. The table displays the **Nickname**, **WWN**, **Operational Status**, **Type**, and **Description** of the device.

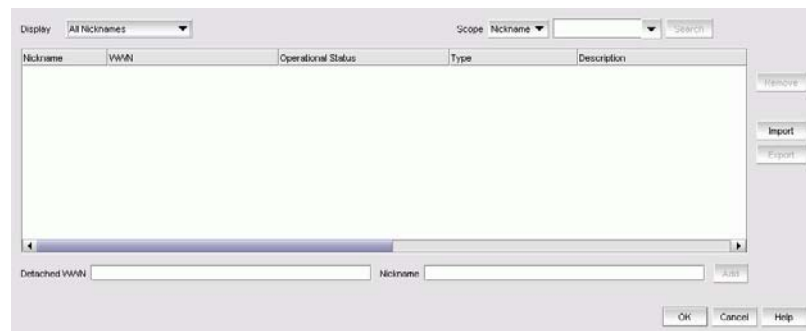
3. Click **OK** to close the **Configure Nicknames** dialog box.

## Searching by Nickname

The SAN Management application allows you to search for objects (switch, fabric, mSAN, product, ports, or N Ports) by nickname.

1. Select **Configure > Nicknames**.

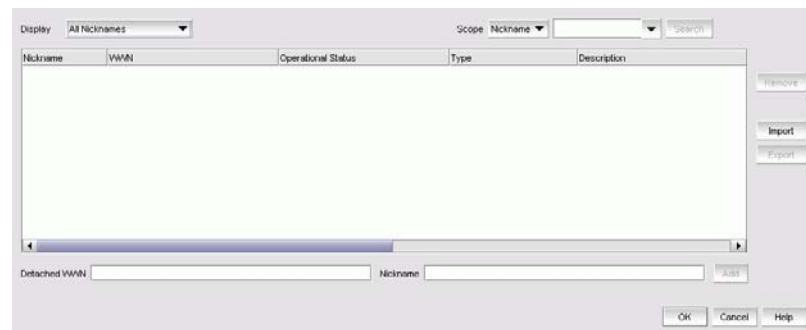
The **Configure Nicknames** dialog box displays (Figure 37).



**FIGURE 38** Configure Nicknames Dialog Box

2. From the **Display** list, select **All Nicknames**.

Only objects with a nickname display.



**FIGURE 39** Configure Nicknames Dialog Box

3. From the **Scope** list, select **Nickname**.
4. Enter the nickname you want to search for in the **Search** field.  
You can search on partial nicknames.
5. Click **Search**.

All devices with the specified nickname (or partial nickname) are highlighted in the **Display** table. You may need to scroll to see all highlighted nicknames.

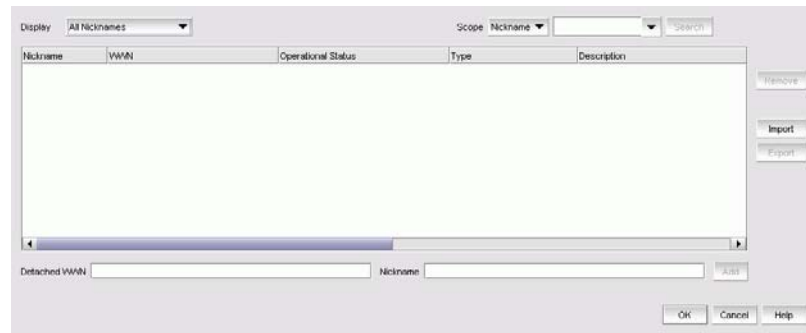
6. Click **OK** to close the **Configure Nicknames** dialog box.

## Searching by WWN

The SAN Management application allows you to search for objects (switch, fabric, mSAN, product, ports, or N Ports) by WWN (world wide name).

1. Select **Configure > Nicknames**.

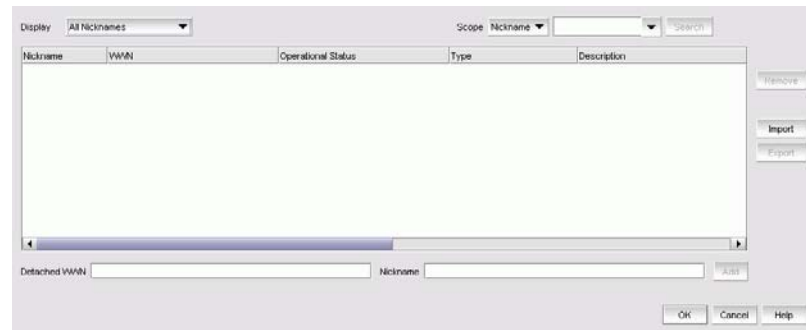
The **Configure Nicknames** dialog box displays (Figure 37).



**FIGURE 40** Configure Nicknames Dialog Box

2. From the **Display** list, select **All WWNs**.

Only objects with a WWN display.



**FIGURE 41** Configure Nicknames Dialog Box

3. From the **Scope** list, select **WWN**.
4. Enter the WWN you want to search for in the **Search** field.

You can search on partial WWNs.

5. Click **Search**.

All devices with the specified WWN (or partial WWN) are highlighted in the **Display** table. You may need to scroll to see all highlighted WWNs.

6. Click **OK** to close the **Configure Nicknames** dialog box.

### Assigning a Nickname to an Existing Device

The SAN Management application allows you to assign a nickname to an existing device.

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays.

2. From the **Display** list, select how you want to display devices.

You can display devices by **All Nicknames**, **All WWNs**, **Only Fabrics And mSANS**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

All discovered devices display.

3. In the **Display** table, select the device to which you want to assign a nickname.

4. Double-click in the **Nickname** column for the selected device and enter a nickname for the device.

If you set nicknames to be unique on the **Options** dialog box and the nickname you entered already exists, the entry is not accepted.

**NOTE:** If you segment a fabric, the Fabric's nickname follows the assigned principal switch.

5. Click **OK** to close the **Configure Nicknames** dialog box.

### Adding a Nickname to a New Device

The SAN Management application allows you to add a new device.

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays.

2. In the **Detached WWN** field, enter the WWN of the device.

3. In the **Nickname** field, enter a nickname for the device.

If you set nicknames to be unique on the **Options** dialog box and the nickname you entered already exists, the entry is not accepted.

4. Click **Add**.

The new device displays in the table.

5. Click **OK** to close the **Configure Nicknames** dialog box.

## Importing Nicknames

This procedure provides step-by-step instructions for importing nicknames from the **Configure Nicknames** dialog box.

If you need to add single (') or a double (") quotation mark to a nickname, you must edit the <Nickname>.csv file using a text editor (such as Notepad). However, by adding single or double quotation marks to the <Nickname>.csv file in an editor other than a text editor, the quotation marks will not display correctly in the SAN Management application.

---

### NOTE

If you add only double quotation marks to a nickname, the SAN management application displays the nickname with two double quotation marks. If you add only single quotation marks, the nickname is displayed as only single quotation marks. If you combine single quotation marks with double quotation marks, however, the application displays the nickname with two single quotation marks.

---



---

### NOTE

The format of the nickname export file changed in EFCM 9.1; therefore, when importing SANavigator or EFCM 8.X or earlier nickname export files and an EFCM 9.1 or later nickname export file, you must import the files separately.

---



---

### NOTE

Do not copy contents from the old export nickname format to the new export nickname format, the nicknames will not import correctly.

---

You can also import nicknames from the Import dialog box, for more information, refer to [“Importing Nicknames”](#) on page 120.

To import nicknames, complete the following steps.

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays.

2. Click **Import**.

The **Import** dialog box displays.

3. From the **Import** list, select **Nicknames**.

4. In the **File Name** field, enter or browse to the nickname file you want to import.

**NOTE:** If you have multiple devices using the same WWN, the nickname associated with the WWN imports to only one of the devices.

5. (Optional) Select one of the following options to set special handling for nicknames assigned to ports:

- For HBA ports, also apply the nickname to the HBA product
- For Storage\* ports, apply one of the nicknames to the Storage product (\*includes product types of Storage, Tape, and Bridge)

6. Click **OK**.

A Warning message displays stating “*Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname. Do you want to continue?*”. Click **OK** to continue.

The file is imported and assigned.

7. Click **OK** to close the **Configure Nicknames** dialog box.

### Importing FC Aliases into Nicknames

This procedure provides step-by-step instructions for importing Zone Alias information from a B model switch into the SAN Management application. from the **Configure Nicknames** dialog box.

To import Zone Alias information from a B model switch into the SAN Management application.s, complete the following steps.

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays.

2. Click **Import**.

The **Import** dialog box displays.

3. From the **Import** list, select **FC Aliases into Nicknames**.

4. In the **Fabric** field, select the fabric from which you want to import FC Aliases.

5. Click **OK**.

A Warning message displays stating “*Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname. Do you want to continue?*”. Click **OK** to continue.

The file is imported and assigned.

6. Click **OK** to close the **Configure Nicknames** dialog box.

### Exporting Nicknames

1. Select **Configure > Nicknames**.

The **Configure Nicknames** dialog box displays.

2. From the **Display** list, select how you want to display devices.

You can display devices by **All Nicknames**, **All WWNs**, **Only Fabrics And mSANs**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

All discovered devices display.

3. Click **Export**.

The **Save** dialog box displays.

4. Browse to the folder where you want to save the file and type a file name in the **File Name** field.
5. Click **Save**.  
The file is exported to the selected folder.
6. Click **OK** to close the **Configure Nicknames** dialog box.

## Removing a Nickname

1. Select **Configure > Nicknames**.  
The **Configure Nicknames** dialog box displays.
2. In the **Display** table, select the nickname of the device you want to remove.
3. Click **Remove**.  
An application message displays asking if you are sure you want clear the selected nickname.
4. Click **Yes**.
5. Click **OK** to close the **Configure Nicknames** dialog box.

## Configuring Enterprise Fabric Mode

---

**NOTE**

Enterprise Fabric Mode is only available on M model fabrics.

---

The **Enterprise Fabric Mode** option is available on the **Configure** menu. This option automatically enables features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. When Enterprise Fabric Mode is enabled, each switch in the fabric automatically enforces a number of security-related features including Fabric Binding, Switch Binding, Insistent Domain IDs, and Domain Register for State Change Notifications (RSCNs).

### About Enterprise Fabric Mode

Activating Enterprise Fabric Mode enables the following features.

- **Fabric Binding.** Allows or prohibits switches from merging with a selected fabric.  
**NOTE:** Fabric Binding cannot be disabled while Enterprise Fabric Mode is active even if the switch is offline.
- **Switch Binding.** This feature, enabled through a product's Element Manager, allows or prohibits switches from connecting to switch E\_Ports and products from connecting to F\_Ports.  
**NOTE:** Switch binding can be disabled while Enterprise Fabric Mode is active if the switch is offline.
- **Domain RSCNs.** This feature, enabled through a product's Element Manager, indicates that an event occurred to a switch in a fabric. The only cause would be a switch entering or leaving the fabric. Notifications are sent fabric-wide and are not constrained by a zone set. Domain RSCNs are not sent between end-products.
- **Insistent Domain ID.** This feature, enabled through a product's Element Manager, sets the domain ID as the active domain identification when the fabric initializes. When Insistent Domain ID is enabled, the switch isolates itself from the fabric if the preferred domain ID is not assigned as the switch's domain ID.

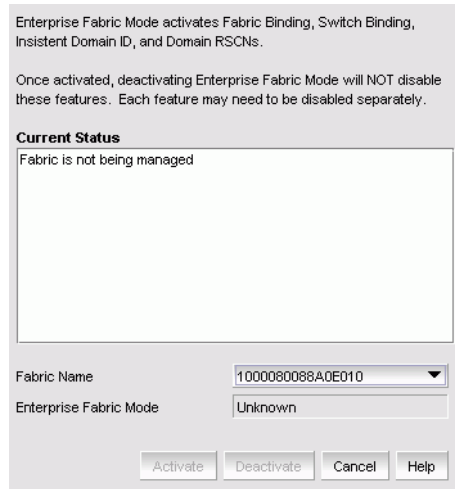
## Setting Enterprise Fabric Mode

### NOTE

Enterprise Fabric Mode is only available on M model fabrics.

1. Select **Configure > Enterprise Fabric Mode**.

The **Enterprise Fabric Mode** dialog box displays (Figure 42).



Enterprise Fabric Mode activates Fabric Binding, Switch Binding, Insistent Domain ID, and Domain RSCNs.

Once activated, deactivating Enterprise Fabric Mode will NOT disable these features. Each feature may need to be disabled separately.

**Current Status**

Fabric is not being managed

Fabric Name: 1000080088A0E010

Enterprise Fabric Mode: Unknown

Buttons: Activate, Deactivate, Cancel, Help

**FIGURE 42** Enterprise Fabric Mode Dialog Box

2. From the **Fabric Name** list, select the fabric for which you want to configure Enterprise Fabric Mode.
3. The fabric's current status displays in the **Enterprise Fabric Mode** field.
4. To activate Enterprise Fabric Mode on the selected fabric, click the **Activate** button.

**NOTE:** You must be managing the fabric to set this option.

5. To deactivate Enterprise Fabric Mode on the selected fabric, click the **Deactivate** button.

**NOTE:** You must be managing the fabric to set this option.

## Configuring Fabric Binding

---

**NOTE**

Fabric Binding is only supported on B model (FOS level 6.0 or higher) and M model manageable switches and fabrics. Fabric Binding in Interop Mode 3 is only supported on FOS level 6.1 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

---

**NOTE**

To enable or disable Fabric Binding in a mixed fabric, at least one B model device and one M model device must be manageable.

---

---

**NOTE**

You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding.

---

The fabric binding feature enables you to configure whether switches can merge with a selected fabric. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

---

---

**NOTE**

When performing fabric binding in an edge fabric with extended discovery disabled on all devices, you must retrieve the translate domain and then enter it into the membership list. You can determine the translate domain using the CLI or enabling extended discovery (temporarily) on any manageable M-model device in the edge fabric.

---

For M model devices, enabling Fabric Binding activates Fabric Binding and enables insistent domain ID. Disabling Fabric Binding on M model devices deactivates Fabric Binding.

For B model devices, enabling Fabric Binding activates Switch Connection Control (SCC) policy and sets Fabric Wide Consistency Policy (FWCP) and insistent domain ID. Disabling Fabric Binding on B model devices deletes SCC policy.

---

---

**NOTE**

In a pure B model fabric, enabling insistent domain ID is not mandatory.

---

## Fabric Binding and Element Manager Switch Binding for Blade Switches

Do not use the Element Manager Switch Binding feature for Blade Switches. You must use the SAN Management application Fabric Binding feature for Blade Switches. The Element Manager Switch Binding does not synchronize with the SAN Management application Fabric Binding. Therefore, if you use both the Element Manager Switch Binding and your SAN Management application Fabric Binding features, you will disconnect the two features.

### *Examples:*

- If you activate an ISL set when a port set is already active, the ISL set takes over and vice-versa.
- If you activate Switch Binding within the Element Manager and then activate Fabric Binding within your SAN Management application, the Fabric Binding is stored by the blade and appended to the current Switch Binding security policy.  
However, after carrying out the above procedure, if you deactivate Fabric Binding within your SAN Management application, it only deactivates on the manageable legacy Switches (refer to [Table 22 Product Icons](#) on page 243). To deactivate the policy on the Element Manager, you must open the Element Manager and deactivate the policy.  
Switch Binding is turned off when the learned fabric policy is merged. To turn Switch Binding back on, you must activate the policy you created within the Element Manager again. Failure to perform this task can lead to a security lapse.
- If Switch Binding is not activated within an Element Manager and Fabric Binding is activated within your SAN Management application, deactivate the Fabric Binding on the Switch that uses your SAN Management application.
- If Switch Binding is activated through an Element Manager and there is an F-Port logged into the Blade that is not in the Switch Binding membership list (for example, an administrator command has not logged out the unwanted port), then Fabric Binding cannot be activated using your SAN Management application.

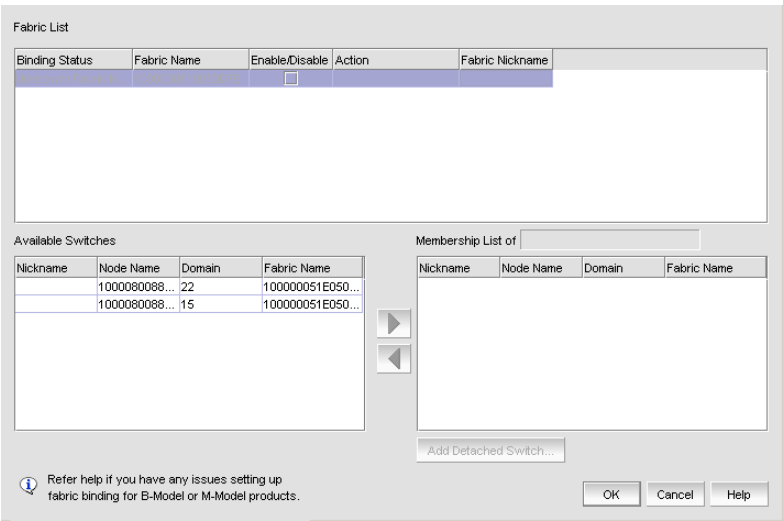
## Enabling Fabric Binding

Fabric Binding is enabled through the **Fabric Binding** dialog box. After you have enabled Fabric Binding, use the **Fabric Membership List** to add switches that you want to allow into the fabric.

**NOTE**

Fabric Binding is only supported on B model (FOS level 6.0 or higher) and M model manageable switches and fabrics. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

1. Select **Configure > Fabric Binding**.  
The **Fabric Binding** dialog box displays ([Figure 43](#)).



**FIGURE 43**    Fabric Binding Dialog Box

2. In the **Fabric List** table, click the **Enable/Disable** check box for fabrics for which you want to configure fabric binding.  
For instructions on adding and removing switches from the membership list, refer to [“Adding Switches to the Fabric Binding Membership List”](#) on page 179 and [“Removing Switches from Fabric Binding Membership”](#) on page 181.
3. Click **OK**.

## Disabling Fabric Binding

Fabric Binding can be disabled while Enterprise Fabric Mode is active if the switch is offline. This disables fabric binding and Enterprise Fabric Mode on the switch, but not the rest of the fabric. Disabled switches segment from the fabric. Fabric Binding is disabled through the **Fabric Binding** dialog box.

---

**NOTE**

Fabric Binding is only supported on B model (FOS level 6.0 or higher) and M model manageable switches and fabrics. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

1. Select **Configure > Fabric Binding**.

The **Fabric Binding** dialog box displays.

2. In the **Fabric List** table, clear the **Enable/Disable** check box for fabrics for which you want to disable fabric binding.
3. Click **OK**.

## Adding Switches to the Fabric Binding Membership List

Once you have enabled Fabric Binding (refer to [“Enabling Fabric Binding”](#) on page 178), you can add switches to the fabric binding membership list.

---

**NOTE**

Fabric Binding is only supported on B model (FOS level 6.0 or higher) and M model manageable switches and fabrics. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

---

**NOTE**

When performing fabric binding in an edge fabric with extended discovery disabled on all devices, you must retrieve the translate domain and then enter it into the membership list. You can determine the translate domain using the CLI or enabling extended discovery (temporarily) on any manageable M-model device in the edge fabric.

---

To add a switch to the fabric, complete the following steps.

1. Select **Configure > Fabric Binding**.

The **Fabric Binding** dialog box ([Figure 43](#)) displays.

2. Select the switches you want to add to the selected fabrics' Fabric Membership List (FML) in the **Available Switches** table.
3. Click the right arrow to move the switches to the **Membership List** table.
4. Click **OK** on the **Fabric Binding** dialog box.

## Adding Detached Devices to the Fabric Binding Membership List

### NOTE

When performing fabric binding in an edge fabric with extended discovery disabled on all devices, you must retrieve the translate domain and then enter it into the membership list. You can determine the translate domain using the CLI or enabling extended discovery (temporarily) on any manageable M-model device in the edge fabric.

To add a switch or SAN router that does not have physical connection and is not discovered to the fabric, complete the following steps.

1. Select **Configure > Fabric Binding**.  
The **Fabric Binding** dialog box displays.
2. Click **Add Detached Switch**.  
The **Add Detached Product** dialog box displays.
3. Select an option from the **Device** list.
4. If you selected **Switch**, complete the following steps.
  - a. Enter the domain ID of the switch in the **Domain ID** field.
  - b. Enter the node WWN of the switch in the **Node WWN** field.
5. If you selected **SANRouter (< 5.0 firmware)**, complete the following steps.
  - a. Enter the R port domain ID of the SAN router in the **R Port Domain ID** field.
  - b. Enter the R port WWN of the SAN router in the **R Port WWN** field.
  - c. Enter the node WWN for domain ID 30 of the SAN router in the **Node WWN for Domain ID 30** field.
  - d. Enter the node WWN for domain ID 31 of the SAN router in the **Node WWN for Domain ID 31** field.
6. If you selected **SANRouter (>= 5.0 firmware)**, complete the following steps.
  - a. Enter the R port domain ID of the SAN router in the **RPort Domain ID** field.
  - b. Enter the R port WWN of the SAN router in the **RPort WWN** field.
  - c. Enter the domain ID of the SAN router in the **Domain ID** field.
  - d. Enter the node WWN of the SAN router in the **Node WWN** field.
7. Click **OK** on the **Add Detached Product** dialog box.
8. Click the right arrow to move the switches to the **Membership List** table.
9. Click **OK** on the **Fabric Binding** dialog box.

## Removing Switches from Fabric Binding Membership

Once you have enabled Fabric Binding (refer to [“Enabling Fabric Binding”](#) on page 178), you can remove switches from the membership list.

---

**NOTE**

Fabric Binding is only supported on B model (FOS level 6.0 or higher) and M model manageable switches and fabrics. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

1. Select **Configure > Fabric Binding**.  
The **Fabric Binding** dialog box ([Figure 43](#)) displays.
2. Select the switches you want to remove from the selected fabrics' Fabric Membership List (FML) in the **Membership List** table.
3. Click the left arrow to move the switches to the **Available Switches** table.  
**NOTE:** If you segment a fabric, the Fabric's nickname follows the assigned principal switch.
4. Click **OK**.

## Port Fencing

Port Fencing allows you to protect your SAN from repeated operational or security problems experienced by ports. Use Port Fencing to set threshold limits (ISL Protocol, Link, and Security) for the number of specific port events permitted during a given time period on the selected object. Port Fencing objects include Fabrics, Directors, Switches (physical), Virtual Switches, Port Types (E Port, F Port, and Fx Port), as well as Ports. Use Port Fencing to directly assign a threshold to these objects. When a switch does not support Port Fencing, a “No Fencing Changes” message displays in the **Threshold** field in the **Ports** table.

If the port generates more events during the specified time period, the SAN Management application blocks the port, disabling transmit and receive traffic until you investigate, solve the problem, and manually unblock the port.


---

### NOTE

Port Fencing displays any existing thresholds discovered on manageable fabrics, directors, and switches running firmware versions M-EOS 7.0 (supports ISL Protocol only) and 8.0 and above (supports ISL Protocol, Link, and Security).

---

Physical fabrics, directors, switches, port types, and ports display when you have the privileges to manage that object and are indicated by the standard product icons. For a list of the product icons, refer to “[Icon Legend](#)” on page 243.

However, virtual switches display when you have the privileges to manage the fabric that contains the virtual switch and are indicated by the virtual icon ().

You can only directly assign thresholds to ports on a virtual switch. To assign a threshold to the virtual switch or its port types, you must assign the threshold to the associated physical switch or to another object above it in the hierarchy. If no thresholds are set above the virtual switch in the hierarchy, the ISL Protocol, Link, or Security Threshold field in the Ports table displays a Limited Fencing Support message.

For more information about port fencing operation when virtual switches are configured, refer to Chapter 1 in the *Open VSANs User Manual*.

## Requirements

To configure port fencing, the following requirements must be met:

- All switches and directors must be one of the following models and must be running firmware M-EOS 7.0 or higher.
  - 12-Port
  - 16-Port, 1 GB
  - 16-Port, 2 GB
  - 16-Port, 4 GB
  - 24-Port, 2 GB
  - 32-Port, 4 GB
  - 64-Port
  - 140-Port
  - 256-Port
- M-EOS 7.X only supports ISL Protocol fencing.
- M-EOS 8.X and above firmware supports ISL Protocol, Link, and Security fencing.
- All switches must be discovered directly using MPI.

## Thresholds

You can create ISL Protocol, Link, and Security thresholds, which you can then assign to available objects in the tree. Thresholds are prioritized using the following policies:

- Port List policies, which have top priority, are assigned to a set of port numbers on a switch and operate no matter what other policies are assigned to the switch.
- Port Type (E Port Type, F Port Type, FL Port Type) policies, which have secondary priority, apply to any port of the Port List policy.
- Default policies, which have the lowest priority, only apply to ports not governed by Port List or Port Type policies.

During the dynamic operation of a SAN, any port could be any type. For example, a technician could disconnect a port from a switch and reconnect that port to a storage port, or the port could change from an E Port to an F Port. Therefore, when calculating the **Affected Ports** value the SAN Management application does not look for the current port type, but looks at the policy priority level in relation to the other policies currently assigned to this switch.

When there are two or more policies on a switch, the total number of **Affected Ports** may be more than the total number of ports on the switch (the same port may adopt different policies depending on changes in the port's port type).

### ISL Protocol Thresholds

Use ISL Protocol thresholds to block a port when one of the following ISL protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation–ISL has repeatedly become segmented.
- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

### Link Thresholds

Use this type of threshold to block a port when a Link Level (Hot I/O) error meets the threshold.

- Link Level (Hot I/O)–Active Loop port repeatedly received LIP. Active non-loop port repeatedly received LR, OLS or NOS.

### Security Thresholds

Use this type of threshold to block a port when one of the following security violations occur:

- Authentication–the switch has repeatedly become unavailable due to authentication events.
- Fabric Binding–the switch has repeatedly become unavailable due to fabric binding events.
- Switch Binding–the switch has repeatedly become unavailable due to switch binding events. Switch Binding is enabled through a product's Element Manager.
- Port Binding–the switch has repeatedly become unavailable due to port binding events.
- ISL Security–(Generic Security Error) the switch on the other side of the ISL detected a specific security violation, but is only able to tell us that a generic security violation has occurred or a security configuration mismatch was detected.
- N Port Connection Not Allowed–the switch has repeatedly become unavailable due to N port connection not allowed events.

## Adding Thresholds

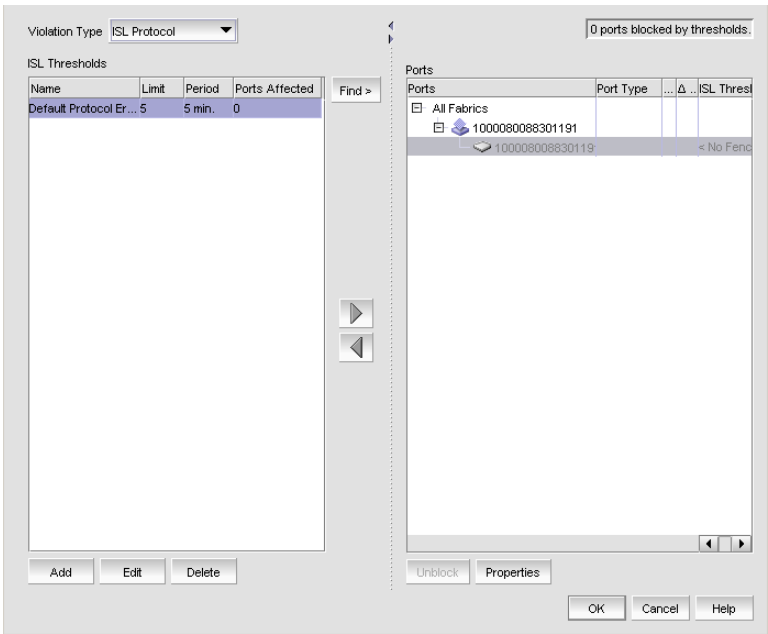
The SAN Management application allows you to add ISL Protocol, Link, and Security thresholds.

### Adding ISL Protocol Thresholds

To add an ISL Threshold, complete the following steps.

1. Select **Configure > Port Fencing**.

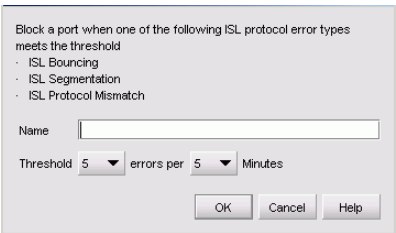
The **Port Fencing** dialog box displays (Figure 44).



**FIGURE 44** Port Fencing Dialog Box

2. From the **Violation Type** list, select **ISL Protocol**.
3. Click **Add**.

The **Add ISL Threshold** dialog box displays (Figure 45).



**FIGURE 45** Add ISL Threshold Dialog Box

4. Enter a name for the threshold in the **Name** field.
5. From the **Threshold errors** list, select the number of port events allowed for the threshold.

6. From the **Threshold Minutes** list, select the time period for the threshold.
7. Click **OK** to add the ISL threshold to the table and close the **Add ISL Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.

8. Click **OK** on the **Port Fencing** dialog box.

## Adding Link Thresholds

To add Link Thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **Link** from the **Violation Type** list.
3. Click **Add**.

The **Add Link Threshold** dialog box displays ([Figure 46](#)).

**FIGURE 46** Add Link Threshold Dialog Box

4. Enter a name for the threshold in the **Name** field.
5. Select the number of port events allowed for the threshold from the **Threshold errors** list.
6. Select the time period for the threshold from the **Threshold Seconds** list.
7. Click **OK** to add the Link threshold to the table and close the **Add Link Threshold** dialog box.  
To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.
8. Click **OK** on the **Port Fencing** dialog box.

## Adding Security Thresholds

To add Security Thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select Security from the **Violation Type** list.
3. Click **Add**.

The **Add Security Threshold** dialog box displays (Figure 47).

The dialog box is titled "Block a port when one of the following security violation types meets the threshold". It contains a list of violation types: Authentication, Fabric Binding, Switch Binding, Port Binding, ISL Security, and N Port Connection Not Allowed. Below the list is a text field labeled "Name". At the bottom, there are two dropdown menus: "Threshold" with the value "5" and "errors per" with the value "5", followed by "Minutes". At the very bottom are three buttons: "OK", "Cancel", and "Help".

**FIGURE 47** Add Security Threshold Dialog Box

4. Enter a name for the threshold in the **Name** field.
5. Select the number of port events allowed for the threshold from the **Threshold errors** list.
6. Select the time limit for the threshold from the **Threshold Minutes** list.
7. Click **OK** to add the Security threshold to the table and close the **Add Security Threshold** dialog box.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.

8. Click **OK** on the **Port Fencing** dialog box.

## Assigning Thresholds

You can assign thresholds to any active object in the **Ports** table. If you assign a threshold to a switch, director, or fabric object, or to the All Fabrics object, the threshold is assigned to all subordinate objects (which do not have a directly assigned threshold) in the tree.

However, if an object inherits a threshold from another object above it in the hierarchy, you cannot remove that inherited threshold directly from the subordinate object. You must either remove the threshold from the higher object to which it was directly assigned or directly assign a different threshold to the subordinate object.

To assign an existing threshold to fabric, director, switch, port type, and port objects, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. From the **Violation Type** list, select a threshold type.
3. From the **Thresholds** table, select the threshold you want to assign.
4. From the **Ports** table, select the objects (All Fabrics, Fabric, Director, Switch, Port Type (Security only), and/or Port) to which you want to assign the threshold.
5. Click the right arrow.

A directly assigned icon ► displays next to the objects you selected in the **Ports** table to show that the threshold was applied at this level and was inherited by every subordinate object below it in the tree (if not affected by lower level direct assignments).

An + icon appears next to every object in the tree to which the new threshold is applied.

6. Click **OK** on the **Port Fencing** dialog box.

## Turning Off Port Fencing Inheritance

When you directly assign a threshold to an object, the threshold is inherited by all subordinate objects (unless it already has a directly assigned threshold) in the tree. You can not remove an inherited threshold from a subordinate object. However, the SAN Management application allows you to effectively turn off inheritance for individual subordinate objects while maintaining inheritance for other subordinate objects. To turn off inheritance for an individual subordinate object, you must create a new threshold with a maximum limit of events allowed and a minimum time period, then assign the new threshold to the subordinate object.

To turn off port fencing inheritance, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. In the **Name** field, type a name for the new threshold (for example, TurnOffISL).
4. From the **Threshold errors/violations** list, select the maximum number of errors or violations allowed.
5. From the **Threshold minutes/seconds** list, select the minimum time period available.
6. Click **OK** on the **Add Threshold** dialog box.
7. Click **OK** on the **Port Fencing** dialog box.

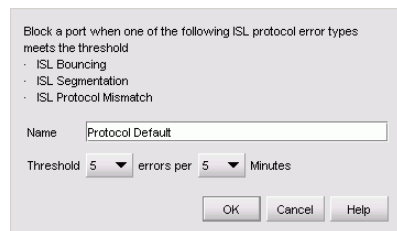
## Editing Thresholds

The SAN Management application allows you to edit the name, number of events needed, and time period of ISL Protocol, Link, and Security thresholds.

### Editing ISL Protocol Thresholds

To edit ISL protocol thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select **ISL Protocol** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.  
The **Edit ISL Threshold** dialog box displays ([Figure 48](#)).



**FIGURE 48** Edit ISL Threshold Dialog Box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Change the number of port events allowed for the threshold from the **Threshold errors** list, if necessary.
6. Change the time period for the threshold from the **Threshold Minutes** list, if necessary.
7. Click **OK** on the **Edit ISL Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.

8. Click **OK** on the **Port Fencing** dialog box.

## Editing Link Thresholds

To edit link thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Link** from the **Violation Type** list.
3. Click **Edit**.

The **Edit Link Threshold** dialog box displays ([Figure 49](#)).

**FIGURE 49** Edit Link Threshold Dialog Box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Change the number of port events allowed for the threshold from the **Threshold errors** list, if necessary.
6. Change the time period for the threshold from the **Threshold Seconds** list, if necessary.
7. Click **OK** on the **Edit Link Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.

8. Click **OK** on the **Port Fencing** dialog box.

## Editing Security Thresholds

To edit security thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select **Security** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

The **Edit Security Threshold** dialog box displays ([Figure 50](#)).



**FIGURE 50** Edit Security Threshold Dialog Box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Change the number of port events allowed for the threshold from the **Threshold errors** list, if necessary.
6. Change the time period for the threshold from the **Threshold Minutes** list, if necessary.
7. Click **OK** on the **Edit Security Threshold** dialog box.

If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

To assign this threshold to fabrics, switches, or switch ports, refer to [“Assigning Thresholds”](#) on page 187.

8. Click **OK** on the **Port Fencing** dialog box.

## Finding Assigned Thresholds

The SAN Management application allows you to find all ports with a specific threshold applied.

To find assigned thresholds, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select a threshold from the **Threshold** table.
4. Click **Find**.
5. Every port which uses the selected threshold is highlighted in the **Ports** table.
6. Click **OK** on the **Port Fencing** dialog box.

## Viewing Thresholds

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Review the **Thresholds** and **Ports** tables.
4. Repeat steps 2 and 3, as necessary.
5. Click **OK** on the **Port Fencing** dialog box.

## Removing Thresholds


When you assign a new threshold to an object, the threshold that was active on that object is automatically removed. The SAN Management application also allows you to remove thresholds from an individual Fabric, Switch, or Switch Port, from all Fabrics, Switches, and Switch Ports at once, as well as from the **Threshold** table.


### Removing Thresholds From Individual Objects

To remove thresholds from the All Fabrics object, an individual Fabric, Switch, or Switch Port, complete the following steps.

1. Select **Configure > Port Fencing**.  
The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. In the **Ports** table, select the object with the threshold you want to remove.
4. Click the left arrow.

**NOTE:** If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. You may assign a different threshold directly to the selected objects or change the assignment on the higher object.

An  icon displays next to every instance where the threshold was removed from an select object, but which now inherits a threshold from higher in the tree.

An  icon displays next to the each select object which does not inherit a threshold from higher in the tree.

5. Click **OK** on the **Port Fencing** dialog box.


## Removing Thresholds From the Thresholds Table

To remove thresholds from all Fabrics, Switches, and Switch Ports as well as the **Threshold** table, complete the following steps.

1. Select **Configure > Port Fencing**.

The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. In the **Thresholds** table, select the threshold you want to remove.
4. Click **Delete**.

A  icon displays next to the selected threshold in the Thresholds table when you click **Delete**.

5. Click **OK** on the **Port Fencing** dialog box.

## Persisting and Unpersisting Fabrics and Switch Groups

Persisting fabrics or switch groups takes a “snapshot” of the current products and connections in the fabric or switch group as a reference point for comparison to future changes. You can export the topology, including persisted fabric or switch group information. Refer to [Exporting Data to Disk or E-mail](#).

---

**NOTE**

If the fabric or switch group’s principal switch changes, the new fabric or switch group must be manually persisted. Persistence does not follow the new fabric or switch group even if only one switch is removed from the original fabric or switch group. The principal switch should always be managed. Also, the principal switch must be a manageable switch or director to administer the devices in the fabric or switch group (refer to [Table 22 Product Icons](#) on page 243).

---

### Persisting a Fabric or Switch Group

To persist a fabric or switch group:

- Select a fabric or switch group in the Physical Map or Product List, then select **Monitor > Persist Fabric**.
- Right-click the fabric or switch group in the Product List or Physical Map and select **Persist Fabric** from the pop-up menu.
- Select a fabric or switch group in the Physical Map or Product List, then click the **Persist Fabric** button on the toolbar.

### Unpersisting a Fabric or Switch Group

To unpersist a fabric or switch group:

- Select a fabric or switch group in the Physical Map or Product List, then select **Monitor > Unpersist Fabrics**.
- Right-click the fabric or switch group in the Product List or Physical Map and select **Unpersist Fabrics** from the pop-up menu.

### Unpersisting a Single Product

You can unpersist a single product in a persisted fabric or switch group if the product is no longer part of the fabric or switch group.

When a product is unpersisted, the connections associated with that product are also removed. The persisted fabric or switch group’s data is updated with the changes.

To unpersist a product, click the product icon and select **Monitor > Unpersist Product**, or right-click the product and select **Unpersist Product** from the menu.

## Graphic Indicators Related to Persisted Fabrics

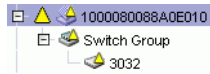
There are various ways to determine the status of persisted fabrics or switch groups and persisted products. Real-time changes to the fabric or switch group display on the Physical Map and the Product List and are listed in the Fabric Log.

### Determining a Persisted Fabric's Status

The fabric or switch group's status is reflected by the indicator that displays on the fabric or switch group on the Physical Map.



**FIGURE 51** Persisted Fabric Icon on Physical Map



**FIGURE 52** Persisted Fabric Icon on Product List

Refer to [Product Status Icons](#) for a list of status icon definitions.

You can also determine changes to the persisted fabric through the Fabric Log.

To display the log, complete the following steps.

1. Select a persisted fabric in the Physical Map or Product List.
2. Select **Monitor > Logs > Fabric Log**.

For more details on the Fabric Log, refer to [“Event Monitoring”](#) on page 216.

3. Click **Close**.

### Determining Status of a Product in a Persisted Fabric

When a product is added to a persisted fabric, it displays with a “plus” icon ([Figure 53](#)).



**FIGURE 53** Product Added to Persisted Fabric

When a product is removed from a persisted fabric, it displays with a “minus” icon ([Figure 54](#)).



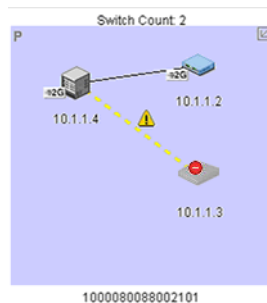
**FIGURE 54** Product Removed from Persisted Fabric

## Determining the Status of Connections in a Persisted Fabric or Switch Group

If more than one connection exists between products and all connections are disconnected, the connections change to yellow, dashed lines. If one or some of the connections are disconnected (but not all), the enabled connections appear as black lines and the disabled connections display as yellow, dashed lines with an interswitch link (ISL) alert. To remove an ISL alert, right-click the connection and select **Clear ISL Alert(s)**. If an ISL is added, the ISL appears as a black line.

### NOTE

In a persisted fabric or switch group, to see ISL Alerts you must set the line type to **Straight** (right-click the group and select **Line Types**, then **Straight**). If the line type is set to **Orthogonal** or **None**, ISL alerts do not appear.



## Clearing ISL Alerts

To clear a single ISL alert, right-click the ISL and select **Clear ISL Alert(s)**.

To clear all ISL alerts, select **Edit > Clear ISL Alert(s)**.

## Merging Persisted Fabrics

When you merge two persisted fabrics, the fabric whose principal switch will be the principal switch in the merged fabric will become the “real” fabric. It will include the switches of both fabrics in the Physical Map and the Product List. The other fabric will become a “ghost” fabric.

On the Physical Map, the ghost fabric displays its original products with “minus” symbols (⊖). On the Product List, the fabric displays as offline and no products display under the fabric. The ghost fabric will not be updated. The Fabric Log is reset after the fabric merge.

## Splitting Persisted Fabrics

When you split persisted fabrics, the principal switch determines which fabric is mapped to the persistent fabric. The fabric that includes the principal switch is mapped to the persistent fabric.

## Layout Changes in Persisted Fabrics

When you move a product in a persisted fabric’s topology, the new positions are stored on the Client. If you log in to the Server from a different Client, you lose the layout of the products if the fabric is not persisted with the layout changes.

## Finding Devices in a Persisted Fabric

When a product is removed from a persisted fabric, it displays a “ghost” image with a minus icon (⊖). Right-click the icon and select **Find Product**. The focus jumps to the online item that corresponds to the “ghost” image from the original fabric.

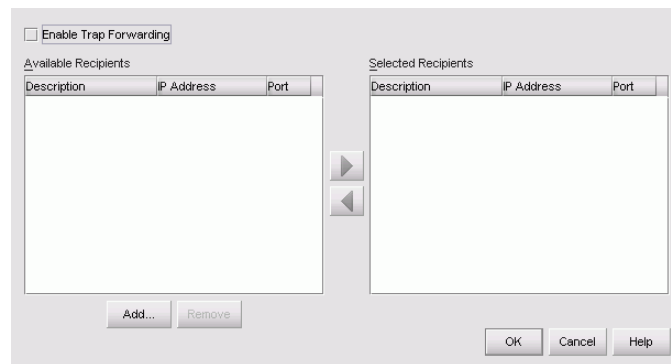
## Configuring Trap Forwarding

Trap forwarding is the process by which you can configure the application to send SNMP traps to other computers. To correctly configure trap forwarding, you must configure the target computer’s IP address and SNMP ports in the **Configure Trap Forwarding** dialog box.

### Configuring Trap Forwarding

1. Select **Monitor > Trap Forwarding**.

The **Configure Trap Forwarding** dialog box displays (Figure 55).



**FIGURE 55** Configure Trap Forwarding Dialog Box

2. If necessary, add or remove trap recipients.  
Refer to [“Adding Trap Recipients”](#) on page 198 and [“Removing Trap Recipients”](#) on page 198 for instructions.
3. In the **Configure Trap Forwarding** dialog box, select the recipient from the **Available Recipients** table and add it to the **Selected Recipients** table by clicking the right arrow.
4. To forward all traps received by the application to the recipients listed in the **Selected Recipients** table, select the **Enable Trap Forwarding** option.
5. Click **OK**.

## Adding Trap Recipients

1. Select **Monitor > Trap Forwarding**.  
The **Configure Trap Forwarding** dialog box displays (Figure 55).
2. Click **Add**.  
The **Add Trap Recipient** dialog box displays (Figure 56).



The dialog box contains the following fields and buttons:

Description	jns	
IP Address	172.0.0.2	Port 162
<input type="button" value="OK"/> <input type="button" value="Cancel"/>		

**FIGURE 56** Add Trap Recipient Dialog Box

3. (Optional) In the **Description** field, enter a description of the trap recipient.
4. In the **IP Address** field, enter the trap recipient's IP address.  
The SAN Management application accepts IP addresses in IPv4 or IPv6 formats.
5. In the **Port** field, enter the trap recipient's TCP/IP port number.  
**NOTE:** The SAN Management application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.
6. Click **OK** on the **Add Trap Recipient** dialog box.
7. Click **OK** on the **Configure Trap Forwarding** dialog box.

## Removing Trap Recipients

1. Select **Monitor > Trap Forwarding**.  
The **Configure Trap Forwarding** dialog box displays (Figure 55).
2. In the **Available Recipients** table, select the recipient you want to remove.
3. Click **Remove**.
4. Click **OK**.

# Configuring Frame Sniffer

## NOTE

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

The frame sniffer feature enables you to count frames passed by a switch port that meet user-specified criteria. You can view, configure, run, and stop tests and their sessions using the **Frame Sniffer** dialog box.

When you run or stop a test through the **Frame Sniffer** dialog box, the application logs the action in the master log file. For more details about information provided in the Master Log, refer to [“Master Log”](#) on page 58.

## Frame Sniffer Requirements

To run Frame Sniffer your switch must meet the following requirements:

- Manageable switch must support Frame Sniffer (M6140 Director, Intrepid 6064 Director, or the Sphereon 3000/4000 series). For a list of manageable switches, refer to [Table 22 Product Icons](#) on page 243.
- Firmware must be M-EOS 5.0 or higher.
- Manageable switch must have an OSMS feature key enabled.
- Manageable switch must run in McDATA fabric mode.
- FC-Host Bus Adapter (HBA) must support in band feature (see table below).

**TABLE 20** FC-Host Bus Adapter Requirements

Host Bus Adapter (HBA) Mfg.	Model	Firmware Level	Windows 2000	Windows XP Pro	Solaris 8/9	Redhat 8/9
Emulex	LP1050DC	v1.90a4	v5-5.10a10-2 b	n/a	v5.02d / v1.6a	
Emulex	LP8000	v3.91a3	v5-5.01a0-1 v1.12.2.0	n/a	v5.02d / v1.6a	n/a
Emulex	LP9002	v3.91a3	v5-5.10a10-2 b	n/a	v6.01f / v/5.0.1e (Solaris 9 only)	n/a
Emulex	LP9002DC	v3.91a3	v5-5.10a10-2 b	n/a	v6.01f	n/a
Emulex	LP9802	v1.81.a1	v5-5.01a0-1 v1.12.2.0	n/a	v5.02d / v1.6a	n/a
JNI	FCE-6410-N	n/a	n/a	n/a	v4.1.5 / v2.0.b.030717-16	n/a
JNI	FCE-6460	v1.5	v5.2/v2.0	n/a	v5.3 / v2.0.b.030717-16	n/a

**TABLE 20** FC-Host Bus Adapter Requirements

Host Bus Adapter (HBA) Mfg.	Model	Firmware Level	Windows 2000	Windows XP Pro	Solaris 8/9	Redhat 8/9
Qlogic	QL-2200	v1.83	v8.1.5.15 / v1.27.13	v8.1.5.12 / v1.27.06	v4.13.01 / v3.05	v6.06.10 / v2.01b5
Qlogic	QL-2202	v1.83	v8.1.5.15 / v1.27.13	v8.1.5.12 / v1.27.06	v4.13.01 / v3.05	v6.06.10 / v2.01b5
Qlogic	QL-2310	v1.43	v9.01.10 / v2.0.02	v9.01.10 / v2.0.02	v4.15.02 / v3.07	v6.06.10 / v2.01b5
Qlogic	QLA-2340	v1.43	v8.2.3.11 / v1.27.23	v8.1.5.12 / v1.27.06	v4.13.01 / v3.05	v6.06.10 / v2.01b5
Qlogic	QLA-2342	v3.03.01	v8.2.3.11 / v1.27.23	v8.1.5.12 / v1.27.06	v4.13.01 / v3.05	v6.06.10 / v2.01b5

## Viewing Frame Sniffer Tests

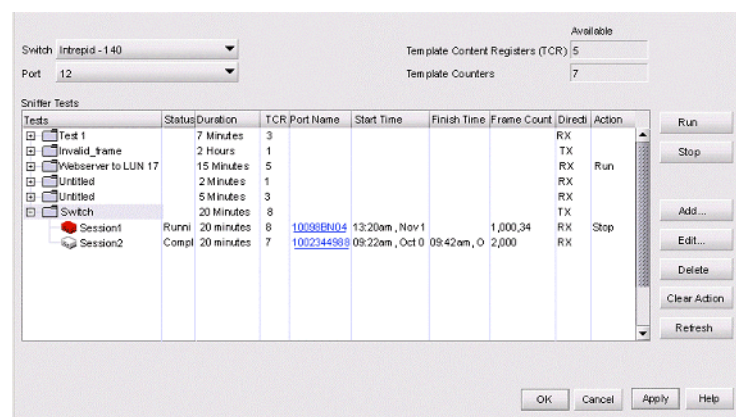
### NOTE

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

You can view and manage frame sniffer tests through the **Frame Sniffer** dialog box.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays ([Figure 57](#)).

**FIGURE 57** Frame Sniffer Dialog Box

2. The configured tests display in the **Sniffer Tests** table.

If you are opening the **Frame Sniffer** dialog box for the first time, the table displays empty. Add new tests using the instructions provided in [“Adding a New Frame Sniffer Test”](#) on page 201.

## Adding a New Frame Sniffer Test

**NOTE**  
Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

You can add tests to count frames passed by a switch port that meet certain criteria.

- 1. Select **Monitor > Frame Sniffer**.  
The **Frame Sniffer** dialog box displays.
- 2. Click **Add**.  
The **New Test** dialog box displays ([Figure 58](#)).

Condition	Mask Value	Word Offset	Match String
NONE	EQ		
NONE	EQ		
NONE	EQ		
NONE	EQ		
NONE	EQ		
NONE	EQ		
NONE	EQ		
NONE	EQ		

**FIGURE 58** New Test Dialog Box

- 3. Type a name for the test.
- 4. (Optional) Type a description for the test.  
This description displays as a tool tip when you point to the name of a test.
- 5. From the **Direction** list, select a direction.  
Some switches only support one direction, in which case you may only have one choice.
- 6. In the **Duration** field, enter the length of time you want the frame sniffer to run.
- 7. Select a condition from the **Condition** list.
- 8. Select a mathematical operator.
- 9. The **Mask Value** and **Word Offset** fields specify criteria that the application uses to find the condition's location in the frame.  
To enter your own values in the **Mask Value** or **Word Offset** fields, select **User Defined** from the **Condition** list.

10. Enter the match string in the **Match String** field.

The match string is the frame value that you are seeking. For example, if you select **Source ID** as the condition and only want to consider source ID of 44FF7R, enter a match string of 44FF7R.

11. Click **OK**.

Your settings are validated. If no issues are found, the new test displays on the **Frame Sniffer** dialog box.

## Running a Frame Sniffer Test

### NOTE

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

You can run tests on a selected switch port.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays.

2. From the **Switch** list, select the switch on which you want to run the test.
3. From the **Port** list, select the switch on which you want to run the test.
4. In the **Sniffer Tests** table, select the tests you want to run.

Press **CTRL** and click to make multiple selections.

5. Click **Run**.

The tests are queued to run and “Run” displays in the **Action** column of the **Sniffer Tests** table for the selected tests.

To undo this action, select the tests and click **Clear Action**. The tests are not run and the **Action** column of the **Sniffer Tests** table displays blank.

6. Click **Apply**.

The Server notifies the switch port to set up the template registers and start monitoring. In the **Sniffer Tests** table, “Running” displays in the **Action** column for the selected tests. Also, a new session displays under each running test. Once the session is finished, an ending time displays in the session’s **Finish Time** column.

7. Click **OK**.

## Stopping a Frame Sniffer Session

---

**NOTE**

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

To stop running sessions, follow these instructions.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays.

2. In the **Sniffer Tests** table, select the running sessions you want to stop.

Press **CTRL** and click to make multiple selections.

3. Click **Stop**.

The sessions are queued to stop and “Stop” displays in the **Action** column of the **Sniffer Tests** table for the selected sessions.

To undo this action, select the sessions and click **Clear Action**. The tests are not run and the **Action** column of the **Sniffer Tests** table displays blank.

4. Click **Apply**.

The session is stopped. In the **Sniffer Tests** table, the **Action** column displays blank for the selected sessions, the **Status** column displays “Stopped”, and the **Finish Time** column displays the time the session was stopped.

5. Click **OK**.

## Editing a Frame Sniffer Test

**NOTE**  
Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

You can edit tests that count frames passed by a switch port that meet certain criteria.

- 1. Select **Monitor > Frame Sniffer**.  
The **Frame Sniffer** dialog box displays.
- 2. Select the test you want to edit.
- 3. Click **Edit**.

The **Edit Test** dialog box displays ([Figure 59](#)).

Name	Test 1			
Description				
Direction	Tx			
Duration	10 Seconds			
Condition	Mask Value	Word Offset	Match String	
NONE	EQ			
NONE	EQ			
NONE	EQ			
NONE	EQ			
NONE	EQ			
NONE	EQ			
NONE	EQ			
NONE	EQ			
OK Cancel Help				

**FIGURE 59**    Edit Test Dialog Box

- 4. Edit the fields as desired.  
Refer to [“Adding a New Frame Sniffer Test”](#) on page 201 for detailed instructions.
- 5. Click **OK**.  
Your settings are validated. If no issues are found, the edited test displays on the **Frame Sniffer** dialog box.

## Deleting a Frame Sniffer Test

---

**NOTE**

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

You can remove tests that count frames passed by a switch port that meet certain criteria.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays.

2. Select the test you want to remove.

**NOTE:** Tests that have running sessions are not deleted.

3. Click **Delete**.

4. Click **OK**.

## Deleting a Frame Sniffer Session

---

**NOTE**

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

You can remove frame sniffer sessions.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays.

2. Select the session you want to remove.

**NOTE:** Running sessions are not deleted.

3. Click **Delete**.

4. Click **OK**.

### Refreshing the Frame Sniffer

---

**NOTE**

Frame Sniffer procedures should only be performed by advanced users and are only available with M-Model manageable switches running M-EOS 5.0 or higher. For a list of manageable devices, refer to [Table 22 Product Icons](#) on page 243.

---

To get the latest information about sessions that displays in the frame sniffer, you should refresh the **Frame Sniffer** dialog box.

1. Select **Monitor > Frame Sniffer**.

The **Frame Sniffer** dialog box displays.

2. Click **Refresh**.

The information for all the running sessions is updated, including finish time, frame count, and session status.

3. Click **OK**.

# Configuring the SNMP Agent

The following sections provide instructions for configuring the SNMP agent.

## Setting Up the SNMP Agent

The simple network management protocol (SNMP) agent instruments the objects defined in the Fibre Channel Management (FCMGMT) Management Information Base (MIB) Version 3.1 and a small number of objects defined in MIB II. Through instrumentation of these MIB objects, the agent acts as a translator of information stored on the Server into a form usable by SNMP management stations.

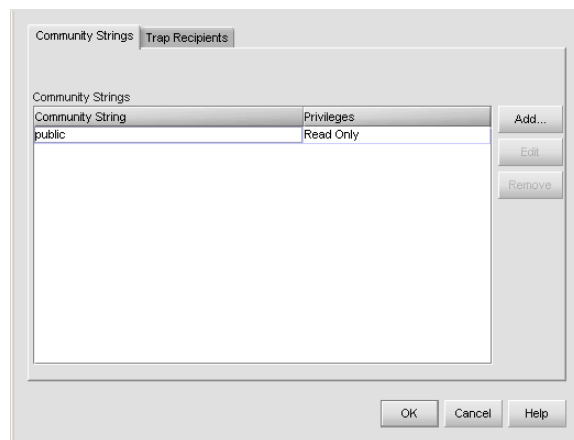
You can configure network addresses and community names for up to 12 SNMP trap recipients, which receive messages through SNMP for specific events that occur on the Server.

To configure the SNMP agent that runs on the Server and implements the Fibre Alliance MIB, use the following steps:

1. Select **Monitor > SNMP Agent > Setup**.

The **SNMP Agent Setup** dialog box displays.

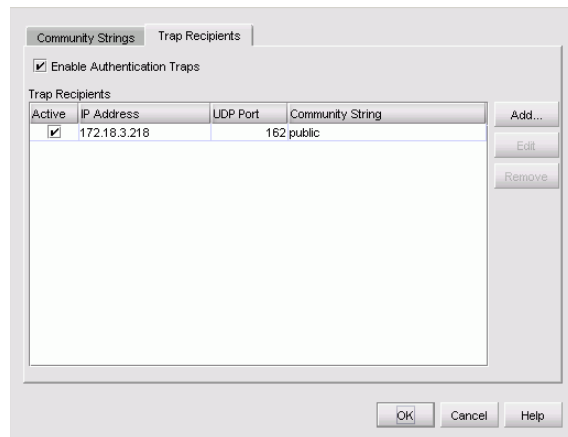
2. In the **SNMP Agent Setup** dialog box, click the **Community String** tab (Figure 60).



**FIGURE 60** SNMP Agent Setup Dialog Box - Community Strings Tab

3. Choose from the following.
  - To add a new community string, click **Add**.  
Refer to [“Adding Community Strings”](#) on page 212 for more instructions.
  - To edit an existing community string, click the recipient’s row in the table and then click **Edit**.  
Refer to [“Editing Community Strings”](#) on page 213 for more instructions.
  - To remove an existing community string, click the community string row in the table and then click **Remove**.
4. In the **SNMP Agent Setup** dialog box, click the **Trap Recipient** tab (Figure 61).

## 5 Configuring the SNMP Agent



**FIGURE 61** SNMP Agent Setup Dialog Box - Trap Recipients Tab

5. To enable or disable authorization traps to be sent when unauthorized management stations try to access SNMP information through the Server, select the **Enable Authentication Traps** check box.
6. Choose from one of the following.
  - To add a new trap recipient, click **Add**.  
Refer to [“Adding Trap Recipients”](#) on page 209 for more instructions.
  - To edit an existing trap recipient, click the recipient’s row in the table and then click **Edit**.  
Refer to [“Editing Trap Recipients”](#) on page 210 for more instructions.
  - To remove a trap recipient, click the recipient’s row in the table and then click **Remove**.
7. Click **OK**.

### Turning On the SNMP Agent

Select **Monitor > SNMP Agent > On**.

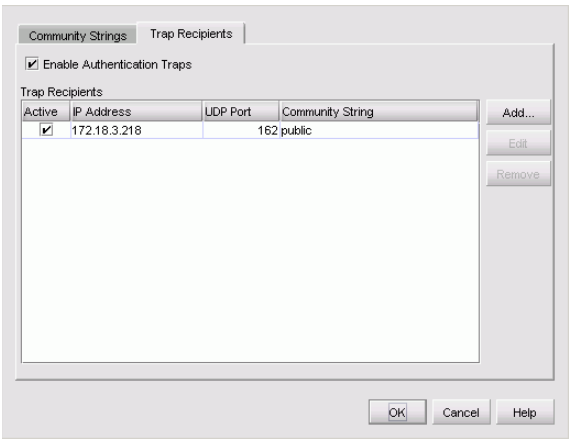
### Turning Off the SNMP Agent

Select **Monitor > SNMP Agent > Off**.

## Adding Trap Recipients

To add a trap recipient during SNMP agent configuration, complete the following steps.

- 1. Select **Monitor > SNMP Agent> Setup**.  
The **SNMP Agent Setup** dialog box displays.
- 2. Click the **Trap Recipient** tab.



**FIGURE 62** SNMP Agent Setup Dialog Box - Trap Recipients Tab

- 3. In the **Trap Recipient** tab, click **Add**.  
The **Add Trap Recipient** dialog box displays.



**FIGURE 63** Add Trap Recipient Dialog Box

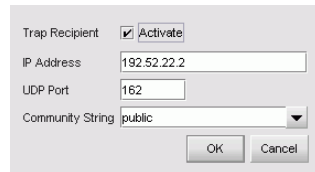
- 4. Select the **Activate** check box to activate the trap recipient.
- 5. In the **IP Address** field, enter the IP Address of the trap recipient.
- 6. To override the default User Datagram Protocol (UDP) port number for a trap recipient with any legal, decimal UDP number, enter the UDP port number in the **UDP Port** field.  
**NOTE:** The SAN Management application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.
- 7. In the **Community String** field, select the trap recipient community.
- 8. Click **OK**.

## Editing Trap Recipients

To edit an existing trap recipient during SNMP agent configuration, use the following steps:

1. Select **Monitor > SNMP Agent> Setup**.  
The **SNMP Agent Setup** dialog box displays.
2. Click the **Trap Recipients** tab.
3. Select the trap recipient you want to edit and click **Edit**.

The **Edit Trap Recipient** dialog box displays (Figure 64).



The screenshot shows a dialog box titled 'Edit Trap Recipient'. It has four main fields: 'Trap Recipient' with a checked 'Activate' checkbox, 'IP Address' with the text '192.52.22.2', 'UDP Port' with the text '162', and 'Community String' with a dropdown menu showing 'public'. At the bottom right are 'OK' and 'Cancel' buttons.

**FIGURE 64** Edit Trap Recipient Dialog Box

4. Edit the trap recipient, as necessary.
    - a. Clear the **Activate** check box to deactivate the trap recipient.
    - b. In the **IP Address** field, edit the IP Address of the trap recipient.
    - c. To override the default User Datagram Protocol (UDP) port number for a trap recipient with any legal, decimal UDP number, enter the UDP port number in the **UDP Port** field.
- NOTE:** The SAN Management application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.
- d. In the **Community String** field, change the trap recipient community.
5. Click **OK**.

## Changing the UDP Port

You can change the User Datagram Protocol (UDP) port number to a trap recipient with any legal, decimal UDP number. To change the UDP port number, complete the following steps.

1. Select **Monitor > SNMP Agent> Setup**.

The **SNMP Agent Setup** dialog box displays.

2. Click the **Trap Recipient** tab.
3. In the **Trap Recipient** tab, click **Edit**.

The **Edit Trap Recipient** dialog box displays.

4. In the **UDP Port** field, enter a new UDP port number.

**NOTE:** The SAN Management application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.

5. Click **OK**.

## Removing Trap Recipients

To remove an existing trap recipient during SNMP agent configuration, use the following steps:

---

### ATTENTION

This procedure removes trap recipients without asking for confirmation.

---

1. Select **Monitor > SNMP Agent> Setup**.

The **SNMP Agent Setup** dialog box displays.

2. Select the trap recipient you want to remove and click **Remove**.

The trap recipient is removed without confirmation.

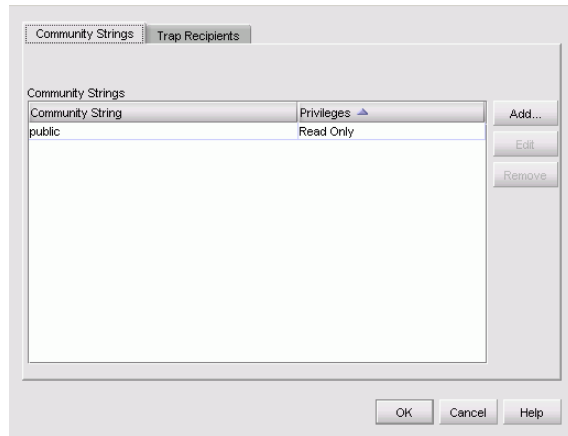
3. Click **OK**.

## Adding Community Strings

To add a community string during SNMP agent configuration, complete the following steps.

1. Select **Monitor > SNMP Agent> Setup**.

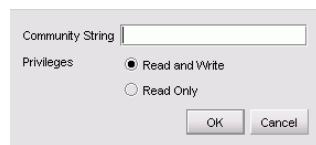
The **SNMP Agent Setup** dialog box displays (Figure 62).



**FIGURE 65** SNMP Agent Setup Dialog Box - Community Strings Tab

2. Click the **Community Strings** tab, if necessary.
3. On the **Community Strings** tab, click **Add**.

The **Add Community String** dialog box displays.



**FIGURE 66** Add Community String Dialog Box

4. Enter a name for the community string in the **Community String** field.
5. Select the appropriate **Privileges** option.

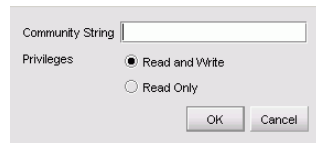
When you select **Read and Write**, an administrator at an SNMP management station has write permissions for writable MIB objects on the Server.

6. Click **OK**.

## Editing Community Strings

To edit an existing community string during SNMP agent configuration, use the following steps:

1. Select **Monitor > SNMP Agent> Setup**.  
The **SNMP Agent Setup** dialog box displays.
2. Click the **Community Strings** tab, if necessary.
3. Select the community string you want to edit and click **Edit**.  
The **Edit Trap Recipient** dialog box displays (Figure 64).



**FIGURE 67** Edit Community String Dialog Box

4. Edit the fields as necessary.  
Refer to [“Adding Community Strings”](#) on page 212 for more details.
5. Click **OK**.

## Removing Community Strings

To remove an existing community string during SNMP agent configuration, use the following steps:

---

### ATTENTION

This procedure removes community string without asking for confirmation.

---

1. Select **Monitor > SNMP Agent> Setup**.  
The **SNMP Agent Setup** dialog box displays.
2. Select the community string you want to remove and click **Remove**.  
The community string is removed without confirmation.
3. Click **OK**.

### Changing the TCP/IP Port for SNMP Trap Events

1. Select **SAN > Options**.

The **Options** dialog box displays.

2. In the **Category** list, select **SNMP Trap Listening**.

The **SNMP Trap Listening** fields display to the right of the **Category** list.

3. In the **Server SNMP Trap Listening Port** field, enter the TCP/IP port number.

**NOTE:** The SAN Management application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.

4. Click **OK**.
5. Restart the application for your changes to take effect.

# Monitoring SAN Products

---

## In this Chapter

This chapter provides instructions for monitoring SAN products using the application.

- Event Monitoring .....216
- Using Event Notification Features .....220
- Creating Reports .....223

## Event Monitoring

The application provides a variety of logs through which you can monitor the SAN. Two daily files are maintained: one that contains events and one that contains summary information. The format of the daily event log file name is Event\_YYYYMMDD.log, where YYYYMMDD is the date that the events took place and the log was created. The daily summary file name format is Event\_YYYYMMDD.sum.

You can view all events that take place in the SAN through the Master Log at the bottom of the main window. You can also view a specific log by selecting an option from the **Monitor** menu's **Logs** submenu. The logs are described in the following list.

- **Audit Log.** Displays a history of user actions performed through the application (except login/logout).
- **Event Log.** Displays errors related to SNMP traps and Client-Server communications.
- **Fabric Log.** Displays the events related to the selected fabric. The event types may include but are not limited to:
  - ISL added to fabric
  - ISL removed from fabric
  - Switch added to fabric
  - Switch removed from fabric
  - Fabric renamed
  - Fabric persisted
  - Fabric status changed
  - Device unpersisted
- **Group Log.** Displays the event logs defined on the Group Management screen.
- **Product Status Log.** Displays operational status changes of managed products.
- **Security Log.** Displays the following security information:
  - Severity
  - User
  - Reason
  - Description
  - Date and Time.
  - Count
  - Category
  - IP
  - Role
  - Interface
- **Session Log.** Displays the users who have logged in and out of the Server.

The application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. For details, refer to [“Using Event Notification Features”](#) on page 220.

For information about the Master Log interface, fields, and icons, refer to [“Master Log”](#) on page 58.

## Viewing Logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only login/logout events (session events), open a specific log through the **View Logs** dialog box.

To view a log, complete the following steps.

1. Select **Monitor > Logs > <log\_type>**.

The **View Logs** dialog box displays the kind of log you selected.

2. Review the information in the log.
3. To clear the log, click **Clear**.
4. Click **Close**.

## Clearing Logs

To clear a log, complete the following steps.

1. Select **Monitor > Logs > <log\_type>**.

The **View Logs** dialog box displays the kind of log you selected.

2. Click **Clear**.
3. Click **Close**.

## Exporting Log Data

You can export the SAN Management application log data in tab-delimited format. This feature is useful for providing the data to a third-party or including it in a report.

To export log data, complete the following steps.

1. Select **Monitor > Logs > <log\_type>**.

The **View Logs** dialog box displays the log for the fabric you selected.

2. Click **Export**.

The **Save <log\_type> Log as** dialog box displays.

3. **Browse** to the folder where you want to save the file and enter a file name in the **File Name** field.
4. Click **Save**.

The file is exported in tab-delimited format. To view it in table format, open the file in Microsoft Excel.

## Deleting Group Logs

To delete a group log, complete the following steps.

1. Select **Monitor > Logs > Group**.  
The **Group Logs** dialog box displays.
2. Select the log you want to delete from the **Group Name** list.
3. Click **Delete Log**.
4. Click **Close**.

## Viewing the Fabric Log

You can view persisted fabric data through the **Fabric Log** dialog box. For more details on the Fabric Log, refer to “[Event Monitoring](#)” on page 216. To display the Fabric Log:

1. Select a persisted fabric in the Connectivity Map or Product List.
2. Select **Monitor > Logs > Fabric Log**.  
The **Fabric Log** dialog box displays.
3. Click **Close**.

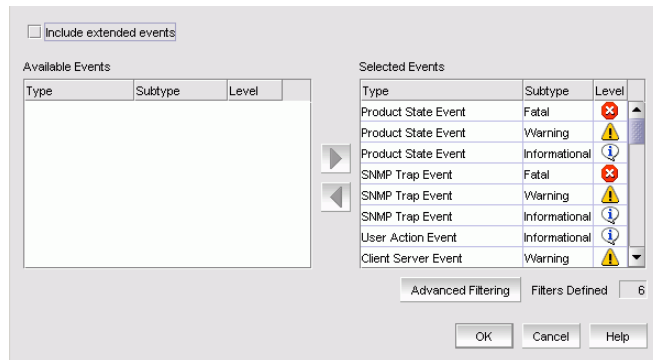
## Filtering Events in the Master Log

You can filter the events that display in the Master Log on the main window. For more information, refer to “[Master Log](#)” on page 58.

### NOTE

The e-mail filter in EFCM is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not be sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

1. On the Master Log, click the **Filter** hyperlink.  
The **Define Filter** dialog box displays ([Figure 68](#)).



**FIGURE 68** Define Filter Dialog Box

2. Select the **Include extended events** check box to include extended events in the log.

3. Include or exclude event types.
  - To include an event type in the filter, select the event from the **Available Events** table and click the right arrow.
  - To exclude an event type from the filter, select the event from the **Selected Events** table and click the left arrow.
4. Click **OK**.
5. On the Master Log, perform one of the following actions.
  - Select **Filter** to view only the events specified in the **Define Filter** dialog box, regardless of the current view.
  - Select **Only events in current view** to view only the events specified in the **Define Filter** dialog box for products in the current view.
  - Clear both the **Filter** and **Only events in current view** check boxes to turn off the filter and view all events.

**NOTE:** Selecting these options only filters product-specific events.

## Copying Log Entries

You can copy data and column headings from logs to other applications. Use this function to analyze or store the data using another tool.

---

### NOTE

When using the **View Logs** dialog box, you can only copy one row at a time. To copy multiple rows of data, copy the data from the Master Log on the main window.

---

## Copying Rows

1. In the log window, select the rows you want to copy.
    - To select contiguous rows, select the first row you want to copy and **Shift**-click in the last contiguous row you want to copy.
    - To select non-contiguous rows, select the first row you want to copy and **CTRL**-click every additional row you want to copy.
  2. Press **CTRL+C** to copy the selected information on the clipboard in tab-delimited format.
  3. Open the application you want to paste the data into.
  4. Click where you want to paste the data.
  5. Press **CTRL+V** (or select the **Paste** command from the other application).
- All data and column headings are pasted.

## Copying the Entire Master Log

1. In the Master Log area, click in the list.
2. Choose **Edit > Select All (CTRL+A)**.  
All Master Log rows are selected.
3. Press **CTRL+C** to copy the selected information in tab-delimited format.
4. In another application, click where you want to paste the data.
5. Press **CTRL+V** (or select the **Paste** command from the other application).  
All data and column headings are pasted.

## Using Event Notification Features

The application records the SAN events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN. You can also configure products to “call home” for certain events, notifying the service center of product problems. For instructions about configuring call home for events, refer to [“Configuring Advanced Call Home”](#) on page 37.

## Configuring E-mail Notification

You can configure the application to send notification of events to users.

1. Select **Monitor > Event Notification > E-mail**.

The **E-mail Event Notification Setup** dialog box displays ([Figure 69](#)).

**FIGURE 69** E-mail Notification Setup Dialog Box

2. Select **Enable E-mail Event Notification**.
3. In the **E-mail Server** field, enter the IP address or the name of the SMTP mail server that the Server can use to send the e-mail.
4. In the **SMTP Port** field, enter the port number of the SMTP mail server.
5. In the **SMTP ID** field, enter the authentication ID of the SMTP mail server.
6. In the **SMTP Password** field, enter the authentication password of the SMTP mail server.

7. In the **Reply Address** field, enter the recipient's e-mail address.
8. In the **Summary Interval** field and drop-down list, enter the length of time the application should wait between notifications.

Notifications are combined into a single e-mail and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

---

**ATTENTION**

Setting too short an interval can cause the recipient's e-mail inbox to fill VERY quickly.

---

9. Select one of the following options:
  - Select **Send to** and enter an e-mail address for a user to send a test e-mail to a specific user.
  - Select **Send to all users enabled for notification** to send a test e-mail to all users already set to receive notification.
10. Click **Send Test E-mail** to test the e-mail server.

A message displays whether the server was found. If the server was not found, verify that the server address was entered correctly and that the server is running. If you are using an SMTP mail server, also verify that the SMTP Port, SMTP ID, and SMTP Password information was entered correctly.
11. To specify which users receive e-mail notification, click **User List**.

The **EFCM 9.7 Server Users** dialog box displays.

  - a. Select the **Filter** check box in the **E-mail** column for each user.
  - b. Click **OK** on the **EFCM 9.7 Server Users** dialog box.
12. Click **OK** on the **E-mail Event Notification Setup** dialog box.

## Enabling Ethernet Events

---

**NOTE**

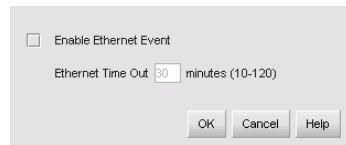
This feature is only available for manageable switches. For a list of manageable products, refer to [Table 22 Product Icons](#) on page 243.

---

An Ethernet event occurs when the Ethernet link between the Server and the managed product is lost. You can configure the application to send notification of Ethernet events.

1. Select **Monitor > Ethernet Event**.

The **Configure Ethernet Event** dialog box displays ([Figure 70](#)).



**FIGURE 70** Configure Ethernet Event Dialog Box

2. Select **Enable Ethernet Event** to be notified when the Ethernet link between the Server and the managed product is lost.
3. In the **Ethernet Time Out** field, enter the number of minutes the application should wait before notifying you of the event.
4. Click **OK**.

## Creating Reports

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following standard report types are available from the **Generate Reports** dialog box:

- **Product List.** Lists the Product List, which has detailed information about the products in the SAN.
- **Operating Status Change.** Lists status change for products in the SAN, including the number of products online and offline, and details about each product's status. Note that this report only looks at the events from the event log for the last 30 days. To save space, the log may be truncated and events lost, resulting in an inaccurate summary. The generation time for the Operating Status Report depends on the size of the event logs for the past 30 days.
- **Performance Data.** Displays the performance data. This report is available for B model and M model devices. Performance Monitoring is a feature of the Advanced Module, which is an Enterprise Edition only optional module. Please contact your sales representative to order the Advanced Module.
- **Connectivity Map.** Displays a graphic of the SAN's topology.
- **Port Usage.** Lists the number of connected ports in the SAN as well as detailed usage information for each port.
- **Fabric Ports.** Lists fabric details including port and director utilization and individual product data.
- **Storage Device Summary.** Lists the assigned and free LUNs for the storage being managed through the application.
- **LUN Masking Summary.** Lists the number of host ports and storage devices in the SAN, as well as the nicknames of hosts with zero assigned LUNs. You must have the LUN Management feature for this report. LUN Management is an optional module available to previous LUN Management licensed customers.
- **Departmental Storage Allocation.** Lists the storage allocation for the entire SAN, the number of servers on the SAN for each department, number of unique LUNs assigned to those servers, the total size of all of those unique LUNs, and a total percentage for each department. You must have the LUN Management feature for this report. LUN Management is an optional module available to previous LUN Management licensed customers.

The following device specific reports are available through the Monitor menu and right-click menus:

- **Consistency.** Requires a SAN router. Compares the configuration of the SAN Routers in a group and highlights the inconsistencies.
- **iFCP Connections and Zones.** Requires a SAN router. Displays all the links in the fabric, which includes the links from both primary and secondary router.
- **LUN Mapping.** Requires a SAN router. Displays LUN information for a selected router.
- **Name Server.** Requires a SAN router. Displays the port information available in the router's Name Server table. If the primary server is available, then the report will be generated based on the primary name server. If not, the report will be generated based on a secondary server (Backup Server).
- **R Port.** Requires a SAN router. Displays configuration information for the SAN Router R\_ports.

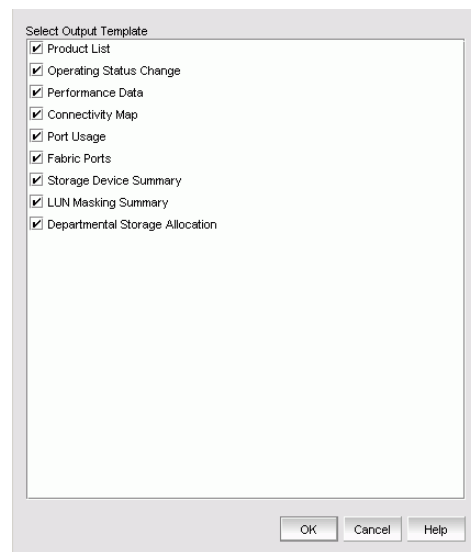
- **Router Configuration.** Requires a SAN router. Displays the following configuration information: System properties, Address configuration, Boot configuration, and Trap configuration.
- **Zone Library.** Requires a zone library be configured for a router, switch, or director. Displays the zoning information of a zone library of the selected device's fabric. The zone library is either a fabric associated library or the global library.

## Generating Reports

You can generate various reports of the SAN. Generated reports are saved to `<Install_Home>\Server\Reports\`.

1. Select **Monitor > Reports > Generate**.

The **Select Template** dialog box displays (Figure 71).



**FIGURE 71** Select Template Dialog Box

**NOTE:** You can also generate a report of the Connectivity Map by clicking **Generate Reports** (or **CTRL+G**) on the right-hand toolbox while viewing a discovered SAN.

2. Select the types of reports you want to generate.

- Product List
- Operating Status Change
- Performance Data
- Connectivity Map
- Port Usage
- Fabric Ports
- Storage Device Summary
- LUN Masking Summary
- Departmental Storage Allocation

3. Click **OK**.

The generated reports automatically display in the **View Reports** dialog box.

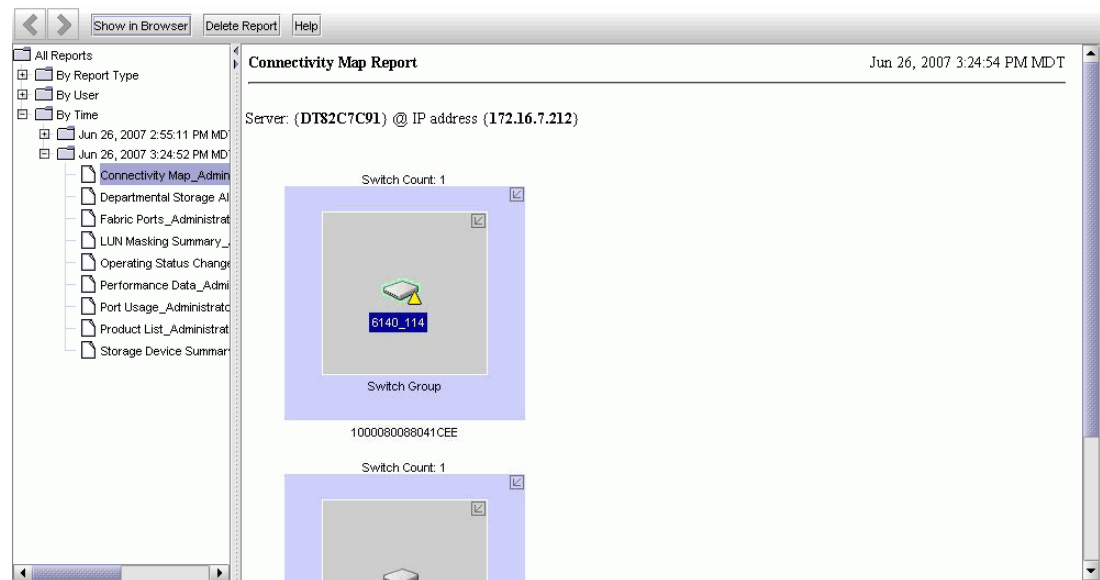
**NOTE:** Hyperlinks in reports are active only as long as the source data is available.

## Viewing Reports

You can view reports through the application, or through an internet browser. Reports are stored in <Install\_Home>\Server\Reports\.

1. Select **Monitor > Reports > View**.

The **Reports** dialog box displays (Figure 70).



**FIGURE 72** View Reports Dialog Box

2. Select the report you want to view in the left pane of the dialog box.

If you do not see the report you want to view, generate it first by following the instructions in [“Generating Reports”](#) on page 224.

- Product List
- Operating Status Change
- Performance Data
- Connectivity Map
- Port Usage
- Fabric Ports
- Storage Device Summary
- LUN Masking Summary
- Departmental Storage Allocation

**NOTE:** Hyperlinks in reports are active only as long as the source data is available.

3. To view the report in your Web browser window, click **Show in Browser**.

The selected report displays in your default Web browser.

4. Click the **Close** button in the Web browser to close.

### Printing Reports

You can print reports through an internet browser. Reports are stored in <Install\_Home>\Server\Reports\.

1. Select **Monitor > Reports > View**.

The **View Reports** dialog box displays.

2. Select the report you want to view in the left pane of the dialog box.

If you do not see the report you want to view, generate it first by following the instructions in [“Generating Reports”](#) on page 224.

**NOTE:** Hyperlinks in reports are active only as long as the source data is available.

3. Click **Show in Browser**.

The selected report displays in your default Web browser.

4. Select **File > Print** (in the Web browser).

The **Print** dialog box displays.

5. Select the printer to which you want to print and click **Print**.
6. Click the **Close** button in the Web browser.
7. Click the **Close** button in the **View Reports** dialog box.

### Printing a Connectivity Map Report

You can print a Connectivity Map report through a photo editor application.

1. Browse to <Install\_Home>\Server\Reports\ and select the Connectivity Map report you want to print.
2. Open the folder of the Connectivity Map report you want to print.
3. Open the image (san.jpg) in a photo editor application.
4. Select **File > Print**.

The **Print** dialog box displays.

5. Select the printer to which you want to print and click **Print**.
6. Click the **Close** button in the photo editor.
7. Click the **Close** button on the **View Reports** dialog box.

## Deleting Reports

You can delete reports using the **View Reports** dialog box.

1. Select **Monitor > Reports > View**.

The **View Reports** dialog box displays.

2. Select the report you want to delete in the left pane of the dialog box.

---

**ATTENTION**

Once you click **Delete Report**, the report is deleted without confirmation.

---

3. Click **Delete Report**.
4. Click the **Close** button in the **View Reports** dialog box.

## Generating Router Reports

Generated reports are saved to <Install\_Home>\Server\Reports\.

1. Select the router for which you want to generate a report.
2. Choose one of the following options:

- Select **Monitor > Reports > <Report\_Type>**.

OR

- Right-click the router and select **Reports > <Report\_Type>**.

The following report types are available.

- Consistency
- iFCP Connections and Zones
- LUN Mapping
- Name Server
- R Port
- Router Configuration
- Zone Library

The selected report automatically displays in the **View Reports** dialog box.

**NOTE:** Hyperlinks in reports are active only as long as the source data is available.

3. To print the report, click **Show in Browser** and complete the following steps.

The selected report displays in your default Web browser.

- a. Select **File > Print** (in the Web browser).

The **Print** dialog box displays.

- b. Select the printer to which you want to print and click **Print**.
- c. Select **File > Close** to close the Web browser.

4. To delete the report, click **Delete Report**.

---

**ATTENTION**

Once you click **Delete Report**, the report is deleted without confirmation.

---

5. Click **Close** to close the **View Reports** dialog box.

### Generating Zone Library Reports

Generated reports are saved to <Install\_Home>\Server\Reports\.

1. Select the device for which you want to generate a zone library report.
2. Choose one of the following options:

- Select **Monitor > Reports > Zone Library**.

OR

- Right-click the device and select **Reports > Zone Library**.

OR

- Select **Configure > Zoning**, then click **Report** on the **Zoning** dialog box.

The zoning report automatically displays in the **View Reports** dialog box.

**NOTE:** Hyperlinks in reports are active only as long as the source data is available.

3. To print the report, click **Show in Browser** and complete the following steps.

The selected report displays in your default Web browser.

- a. Select **File > Print** (in the Web browser).

The **Print** dialog box displays.

- b. Select the printer to which you want to print and click **Print**.

- c. Select **File > Close** to close the Web browser.

4. To delete the report, click **Delete Report**.

---

**ATTENTION**

Once you click **Delete Report**, the report is deleted without confirmation.

---

5. Click **Close** to close the **View Reports** dialog box.

# Troubleshooting

---

## In this Appendix

This appendix provides troubleshooting information.

- *Problems with Addresses*.....229
- *Problems with Discovery*.....230
- *Problems with Fabric Binding*.....233
- *Problems with LUNs* .....233
- *Problems with Products* .....234
- *Miscellaneous Problems*.....234

## Problems with Addresses

Problem	Resolution
No subnets or addresses selected.	<ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>Out-of-Band</b> tab.</li> <li>3. Click on the subnet or individual address you would like to discover in the <b>Available Addresses</b> pane.</li> <li>4. Click the appropriate right arrow to move your choice to the <b>Selected Subnets</b> pane, or to the <b>Selected Individual Addresses</b> pane.</li> <li>5. Click <b>OK</b>.</li> </ol>
Wrong IP addresses selected.	<ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>Out-of-Band</b> tab.</li> <li>3. Verify that the IP addresses in the <b>Selected Subnets</b> and <b>Selected Individual Addresses</b> panes are the correct current addresses for the SAN.</li> <li>4. Click <b>OK</b>.</li> </ol>
Wrong community strings are selected.	<ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>Out-of-Band</b> tab.</li> <li>3. Select an IP address.</li> <li>4. Click <b>Change</b>.</li> <li>5. Select the desired community strings.</li> <li>6. Click <b>OK</b>.</li> </ol>

## Problems with Discovery

Problem	Resolution
An indirectly discovered device does not display correctly (for example, a NPIV host displays as a loop of HBAs).	Make sure you enter all IP addresses in Discovery to view proper device icons in the topology.
Attempting to discover an Mi10K Director displays “Too many sessions” and “No response” statuses.	Verify that no other EFCM application is currently discovering the Mi10K Director. Remove the Mi10K Director IP Address from all other EFCM application Discover Setup dialogs. The Mi10K Director will not display in the current topology if any other EFCM application is discovering the Director.
Broadcast request blocked by routers.	<p><b>Resolution 1:</b> If you know the IP addresses and the addresses are not in the <b>Available Addresses</b> pane:</p> <ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>Out-of-Band</b> tab.</li> <li>3. Click <b>Add</b>.</li> <li>4. Enter data in the dialog box.</li> <li>5. Click <b>OK</b>.</li> <li>6. Repeat steps 1 through 5 until all your addresses are available.</li> <li>7. Select the IP addresses you would like to discover in the <b>Available Addresses</b> pane.</li> <li>8. Click the right arrow to move your choices to the <b>Selected Individual Addresses</b> pane.</li> <li>9. Click <b>OK</b>.</li> </ol> <p><b>Resolution 2:</b> If you know the IP addresses and the addresses are listed in the <b>Available Addresses</b> pane:</p> <ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>Out-of-Band</b> tab.</li> <li>3. Select the IP addresses you would like to discover in the <b>Available Addresses</b> pane.</li> <li>4. Click the right arrow to move your choices to the <b>Selected Individual Addresses</b> pane.</li> <li>5. Click <b>OK</b>.</li> </ol>
Cannot open an Element Manager for a device.	Ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application should be used to monitor and manage the same devices in a subnet.
Cannot see HBA in Discovery Setup dialog box.	EFCM requires specific HBA driver levels. Verify the driver levels.
Devices are not being discovered.	Ensure that your SNMP communication parameters are set correctly to discover manageable switches. For a list of manageable products, refer to <a href="#">Table 22 Product Icons</a> on page 243.
Devices cycle between online and offline.	<ol style="list-style-type: none"> <li>1. Select <b>SAN &gt; Options</b>.</li> <li>2. Select the <b>SNMP Discovery</b> (under <b>Software Configuration</b>).</li> <li>3. Increase the value in the <b>SNMP Timeout</b> field.</li> <li>4. Select the <b>Apply settings to all currently defined IP addresses</b> check box.</li> <li>5. Click <b>OK</b>.</li> </ol>

Problem	Resolution
Discovered devices are not being displayed.	<p>To correctly discover all SAN devices, specify each device in the <b>Out-of-Band</b> dialog box, either by the individual IP address or by subnet.</p> <ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>General</b> tab.</li> <li>3. Select the <b>Out-of-Band Discovery</b> check box.</li> <li>4. Select the <b>Out-of-Band</b> tab to specify the IP addresses you want to discover through out-of-band discovery.</li> <li>5. Add, change, and remove IP addresses, as necessary. Refer to <a href="#">“Configuring Address Properties”</a> on page 142 for instructions.</li> <li>6. Select IP addresses from the <b>Available Addresses</b> table and add them to the <b>Selected Subnets</b> or <b>Selected Individual Addresses</b> tables by clicking the appropriate right arrow.</li> </ol> <p><b>NOTE:</b> If you change the password on the Switch or Director, you must enter the new password during discovery on the <b>Product Type and Access</b> tab of the <b>Address Properties</b> dialog box.</p> <ol style="list-style-type: none"> <li>7. Click <b>OK</b>.</li> </ol>
	Ensure that you've selected to view the fabric that includes the discovered devices.
	Ensure that only one copy of the application is being used to monitor and manage the same devices in a subnet.
Discovery is not enabled.	<ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>.</li> <li>2. Select the <b>General</b> tab.</li> <li>3. Select either the <b>Out-of-Band Discovery</b> check box or the <b>In-Band Discovery</b> check box, or both. Refer to <a href="#">“Setting Up Discovery”</a> on page 139 for instructions.</li> <li>4. Click <b>OK</b>.</li> </ol>
Discovery is turned off.	Select <b>Discover &gt; On</b> .
Discovery of a Cisco 5428 device failed.	This product may not respond to broadcast discovery. Add the specific IP Address of the device to the <b>Selected Individual Addresses</b> table of the <b>Discover Setup</b> dialog box to discover the device. Refer to the related Help or user manual for more information.
Discovery of a SAN Router device failed.	<p><b>Reason 1:</b> Inband IP address of the SAN Router has not been setup. This can occur after user sets the SAN Router to factory defaults.  <b>Workaround:</b> Set the inband IP address to a valid value.</p> <p><b>Reason 2:</b> SNS not initialized in the firmware. This can occur in older Eclipse SAN Routers (3300 and 4300) if all ports are set to gigE (non iSCSI and non iFCP) and there are no FC ports. Also, the FC task in the SAN Router can fail to initialize and the SNS task will not start.  <b>Workaround:</b> None - contact Brocade technical support.</p> <p><b>Reason 3:</b> Bad VPD setup (non-Brocade SAN Router WWN).  <b>Workaround:</b> None - contact Brocade technical support.</p>

# A In this Appendix

Problem	Resolution
Discovery of a Blade Switch may not work if the admin password has been changed from the default.	<p>In order for EFCM to discover and manage Blade Switches, the user and password values must match the values in the Element Manager. If the user and/or password values are changed within the Element Manager, the settings in discovery must also be changed.</p> <p><b>NOTE:</b> For Blade Switches, the default user is “admin” and default password is “password”.</p> <p>To set the user and password for the Blade Switch, complete the following step.</p> <ol style="list-style-type: none"> <li>1. Select <b>Discover &gt; Setup</b>. The <b>Discover Setup</b> dialog box displays.</li> <li>2. Click the <b>Out-of-Band</b> tab.</li> <li>3. Click <b>Add</b>. The <b>Address Properties</b> dialog box displays.</li> <li>4. Click the <b>Product Type and Access</b> tab.</li> <li>5. Select <b>Switch</b> from the <b>Product Type</b> list.</li> <li>6. In the <b>User ID</b> field, enter a user ID.</li> <li>7. In the <b>Password</b> and <b>Retype Password</b> fields, enter the password.</li> <li>8. Click <b>OK</b> on the <b>Address Properties</b> dialog box.</li> <li>9. Click <b>OK</b> on the <b>Discover Setup</b> dialog box.</li> </ol>
Discovery time is excessive.	<ol style="list-style-type: none"> <li>1. Select <b>SAN &gt; Options</b>.</li> <li>2. Select the <b>SNMP Discovery</b> (under <b>Software Configuration</b>).</li> <li>3. Decrease the value in the <b>SNMP Timeout</b> field.</li> <li>4. Select the <b>Apply settings to all currently defined IP addresses</b> check box.</li> <li>5. Click <b>OK</b>.</li> </ol>
The symapi.jar file is not in the class path.	Verify that the symapi.jar file has been copied into EFCM's directory.

## Problems with Fabric Binding

Problem	Resolution
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You may have attempted to disable Fabric Binding through the <b>Fabric Binding</b> dialog box while Enterprise Fabric Mode was enabled. Disable the Enterprise Fabric Mode through the <b>Enterprise Fabric Mode</b> dialog box before disabling Fabric Binding.
Fabric Binding failed because data cannot be populated to the switch.	<p>The following list provides the possible causes of Fabric Binding failure:</p> <ul style="list-style-type: none"> <li>• Fabric is busy or is rebuilding.</li> <li>• Switch is busy.</li> <li>• Insistent Domain ID is not checked for all switches in the fabric.</li> <li>• Firmware doesn't support Fabric Binding (SAN Routers with firmware below version 4.7, non-manageable switches). For a list of manageable products, refer to <a href="#">Table 22 Product Icons</a> on page 243.</li> <li>• Network failure.</li> <li>• Switch is undergoing firmware upgrade/downgrade or NDCLA (Non disruptive Code Load Activation).</li> <li>• Switch is offline.</li> <li>• Binding feature not licensed.</li> <li>• B model switch ACL Connection Control Policy is set to NOT accept distribution.</li> <li>• B model switch discovered using invalid credentials.</li> </ul>

## Problems with LUNs

Problem	Resolution
The application cannot currently manage LUNs on this device.	<p>Verify the following conditions have been met:</p> <ul style="list-style-type: none"> <li>• Check the discovery setup.</li> <li>• Verify that discovery is not still in progress.</li> <li>• Verify that the management application is installed in the appropriate path.</li> <li>• Verify that the device you've selected is a supported device configuration.</li> <li>• Verify that the device is on-line.</li> <li>• Verify that the management server is running.</li> </ul>
Communication with the storage management application failed.	<p>Verify the following conditions have been met:</p> <ul style="list-style-type: none"> <li>• Verify that the device is on-line.</li> <li>• Verify that the management server is running.</li> </ul>
LUN Management actions failed.	<p>Verify the following conditions have been met:</p> <ul style="list-style-type: none"> <li>• Verify that the device is on-line.</li> <li>• Verify that the management server is running.</li> <li>• Verify that the Client is communicating with the Server.</li> <li>• Verify that a green Server connection indicator displays on the status bar.</li> <li>• Verify that the LUN data configuration was not changed while the dialog box was open.</li> </ul>

## Problems with Products

Problem	Resolution
Adding a port to a storage array also adds all ports associated with its discovered node.	Check all associated ports to determine if they should be added to the storage array.
Cannot disable Fabric Binding while Enterprise Fabric Mode is active.	You may have attempted to disable Fabric Binding through the <b>Fabric Binding</b> dialog box while Enterprise Fabric Mode was enabled. Disable the Enterprise Fabric Mode through the <b>Enterprise Fabric Mode</b> dialog box before disabling Fabric Binding.
Enabling secure socket shell (SSH) service errors.	This feature is dependent on having the Element Manager feature installed. If the error message, “received error in attempt to release admin privileges - reason: no response” displays while configuring the SSH service for Switch Blades using Element Manager, you must install the Blade Switch Element Manager.
HBAs not connected to SAN.	Check your physical cables and connectors.
Switches not connected to Ethernet.	Check your physical cables and connectors.
Switches not connected to SAN.	Check your physical cables and connectors.

## Miscellaneous Problems

Problem	Resolution
Cannot delete text in Telnet session window in Linux system	On Linux systems, you must use <b>CTRL + BACKSPACE</b> to delete text in the Telnet session window.
“Code Execution Error: Array Index Out-Of-Bounds” displays.	Retry the command or action. If the problem persists, contact Customer Support.
“Code Execution Error: Internal Exception” displays.	Retry the command or action. If the problem persists, contact Customer Support.
“Code Execution Error: Invalid Product Type” displays.	Retry the command or action. If the problem persists, contact Customer Support.
“Code Execution Error: Missing Property File” displays.	Retry the command or action. If the problem persists, contact Customer Support.
CSV data imported incorrectly.	When entering information directly into a CSV file, make sure you only use commas (,) to separate attributes. For example, if you enter 1000080088520000,Brocade Communications Systems, Inc.,v2.4.1c 123 into a CSV file for Node Name, Vendor, and Firmware 1000080088520000 displays as the Node Name, Brocade Communications Systems displays as the Vendor, Inc. displays as the Firmware, and v2.4.1c 123 does not display.

Problem	Resolution
Data and settings not imported during installation.	Open an MS-DOS window and enter the following script at the command line: Install_Service <startstatus> <runnow>  where startstatus parameter is <b>manual</b> or <b>auto</b> and runnow parameter is <b>true</b> or <b>false</b>
Error occurs when trying to delete a nickname.	Once assigned, a nickname cannot be deleted and left blank.
An indirectly connected device does not display.	Make sure you have the SANtegrity Authentication PFE key enabled.
An indirectly discovered IBM host displays as a storage device.	Make sure you enter all IP addresses in Discovery to view proper device icons in the topology.
Mapping a loop to a hub causes the loop group and the outermost portion of the topology's background group color or layout format to revert to the default.	Make the background and/or layout changes after mapping the loop to the hub.
Need more information about features.	Many of the features described in this document are explained in more detail in other manuals or Help modules. Search the online Help or refer to the related user manual for more information. To find all the help topics that contain a particular word or phrase: 1. On the <b>Help</b> window, click the tab with the magnifying glass icon. 2. In the <b>Find</b> field, enter the word or phrase for which you want to search. 3. Press <b>Enter</b> .
Product will not install on a Windows system.	Verify that the system has 100 MB available on the C drive. The program requires 100 MB for installation, but only 50 MB to run.
Receiving error "Compatibility between <TARGET VERSION> and <CURRENT VERSION> is unknown. Do you want to continue?"	Firmware files are included in the upgrade process, but release rules are not. Since release rules are required when sending another firmware version to a switch, this error results. To fix this problem, add the latest firmware file to the firmware library. This also adds the new release rules and resolve the problem.
Remote client login fails when you login using the Server IP Address in the <b>Network Address</b> field for remote client 1 and then try to login using the Network Name in the <b>Network Address</b> field for remote client 2.	When logging into remote clients, login is based on first time input, therefore, whichever login type (Server IP Address or Network Address) you choose for the first time login is the only login type allowed for all future login attempts.
Server to Client communication is inhibited.	In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but is immediately logged out because the Server cannot reach the Client. To resolve this issue, the application automatically detects the network configuration and run the Client in "polling mode" when necessary. When the Client is not running in polling mode, the Server calls the client whenever it has new data.

## A In this Appendix

Problem	Resolution
Server doesn't seem to be starting.	Examine the Server log (<Install_Home>\Server\Universe_Home\TestUniverse\_Working\EventStorageProvider\Event_YYYYMMDD.log) for diagnostic information.
System reboots or is unable to gather SNMP information.	Multiple SNMP calls are being sent to a device that can't handle the constant requests for information. To resolve this issue, verify that the devices you are discovering are not being discovered by another Server. Discovering devices using multiple Servers may result in errors.
System response time sluggish when backup occurs.	If system response time becomes extremely sluggish, check the event log directory (<Install_Home>\Server\Universe_Home\TestUniverse\_Working\EventStorageProvider). If it contains large log files (more than 50,000 KB), delete or move all except the current day's log files.
Using Fabric Manager or Device Manager to manage Cisco MDS9xxx switches.	Install JRE 1.4 or greater, which includes Java Web Start.
Windows service does not display correctly in the Computer Management (Windows 2000) or Service Control Manager (Windows NT) window.	If you installed or uninstalled the Win32 service while the <b>Computer Management</b> or <b>Service Control Manager</b> window was open, the service does not display. Close the window and re-open it to see the changes.
The zoning method is not supported.	You are trying to set zoning methods that produce invalid zones. For example, the application does not permit you to set a domain/port or fabric address zone in an interoperable manageable fabric because it would create an invalid zone.

# Editing Configuration Properties Files

---

## In this Appendix

This appendix provides instructions for updating the configuration properties file.

- *Specifying a Host IP Address in Multi-NIC Networks.....238*
- *Editing Master Log Settings.....238*

## Specifying a Host IP Address in Multi-NIC Networks

When you have multiple network card server/hosts (two cards in the same machine), you must configure the trap event distributor to know which network card it should listen to for receiving traps.

To change the IP address, you need to edit the *smp.server.edipaddress* variable to instruct the trap event distributor to use a specific IP address.

To specify an IP address for the trap event distributor, complete the following steps.

1. Open the <Install\_Home>\resources\Server\config.properties file using a text editor (for example, Notepad).
2. Add the following line:  

```
smp.server.edipaddress=x.x.x.x
```

 (where x.x.x.x is the desired IP Address)
3. Save the file and restart the server.

## Editing Master Log Settings

The application keeps a log of events that occur in the SAN. By default, the event history is kept for 45 days, until 100 MB of disk space is taken up, or when the number of entries reaches 2000.

You can manually change the retention period and the disk space usage assigned to entries in the Master Log. For a list of the editable parameters, refer to [Table 21](#).

**TABLE 21** Master Log Parameters

Type	Default	Minimum	Maximum
Log Retention Days	45 days	1 day	365 days
Log Disk Space	1000 MB	1 MB	4096 MB

To edit the master log settings, complete the following steps.

1. Open the <Install\_Home>\resources\Server\config.properties file using a text editor (for example, Notepad).
2. Add the following lines:  

```
# Maximum space reserved for the log (where xx is a value between 1MB and 1024MB, inclusive)
smp.log.maxLogDiskSpace=xx
# Maximum number of days to retain the log (where xx is the number of days between 1 and 365 to retain the log)
smp.log.maxLogRetentionDays=xx
```
3. Save the file and restart the server.

## Configuring the ECCAPI Port Number

To change the ECCAPI port number, complete the following steps.

1. Open the <Install\_Home>\resources\Server\config.properties file using a text editor (for example, Notepad).
2. Go to the following line:

```
smp.server.ecc.api.export.port=xxxxx  
(where xxxxx is the current port number)
```

3. Change the port number.
4. Save the file and restart the server.

## Configuring the CLI Proxy Listening Port Number

To change the ECCAPI port number, complete the following steps.

1. Open the <Install\_Home>\resources\Server\config.properties file using a text editor (for example, Notepad).
2. Go to the following line:

```
smp.server.cliProxyListeningPort=xxxxx  
(where xxxxx is the current port number)
```

3. Change the port number.
4. Save the file and restart the server.

## **B** In this Appendix

# Reference

---

## In this Appendix

This appendix provides useful reference information.

- *Compatibility with Other Applications* .....242
- *Changing the TCP/IP Port for SNMP Trap Events*.....242
- *Icon Legend* .....243
- *Keyboard Shortcuts*..... 247

## Compatibility with Other Applications

The application is designed to operate smoothly with other Enterprise applications and network-monitoring programs. Because this application has fully configurable SNMP trap listening and forwarding functions, it can act as a primary or secondary network manager. It can listen for trap events on any port and can forward traps to other network management software, enabling easy integration into existing systems.

Only one software application can control a TCP/IP port at a given time. If the application is not the primary network management tool and you plan to run the application on the same computer, you may need to reconfigure the application to listen for traps on a different port. For instance, if the primary network management software is configured to listen for traps on port 162 and forward them on port 3000, reconfigure the application to listen for traps on port 3000.

## Changing the TCP/IP Port for SNMP Trap Events

1. Select **SAN > Options**.  
The **Options** dialog box displays.
2. In the **Category** list, select **SNMP Trap Listening**.
3. In the **SNMP Listening Port #** field, change the SNMP listening port number to the new number.
4. Click **OK**.

**NOTE:** Changes to this option take effect after a application reboot.

5. Restart the application for your changes to take effect.

To forwarding SNMP traps to other applications, refer to [“Configuring Trap Forwarding”](#) on page 197.





















# Icon Legend

Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Connectivity Map.



















## Product Icons

The following table lists the manageable SAN product icons that display on the topology. Some of the icons shown in [Table 22](#) only display when certain features are licensed. When a manageable product is administered by another Server, the Generic icon displays.

**TABLE 22** Product Icons




















Icon	Description	Icon	Description
	Sphereon 3016 Switch		Sphereon 3032 Switch
	Sphereon 3216 Switch		Sphereon 3232 Switch
	Sphereon 4300 Switch		Sphereon 4710 Switch
	Sphereon 4400 Switch		Sphereon 4500 Switch
	M4700F Switch		B model Switch
	Intrepid 6064 Director		B model Director
	M6140 Director		Mi10K Director
	Mi10K Director Partition		Mi10K Director Partition - Disabled
	SAN Router		Generic Brocade Switch, Director, or Access Gateway
	ES-1000 Switch		ED-5000 Director

**TABLE 22** Product Icons (Continued)

Icon	Description	Icon	Description
	ASM Switch		Blade Switch
	Bridge		Director
	FCIP Bridge or Gateway		Host
	Host Bus Adapter (HBA)		Hub
	iSCSI Device		iSCSI Bridge or Gateway
	JBOD		JDISK
	Loop		Network Attached Storage (NAS)
	Server		Storage
	Tape		Unknown










## Group Icons

**TABLE 23** Group Icons

Icon	Description	Icon	Description
	Bridge		Enclosure
	Fabric		FCIP Bridge or Gateway
	Host		iSCSI
	iSCSI Bridge or Gateway		iSCSI Device
	Isolated		Loop
	mSAN		Routed In
	Routed In Fabric		Routed In Router Fabric
	SAN Router		Storage
	Switch		Tape
	Virtual Device		

## Product Status Icons




**TABLE 24** Product Status Icons

Icon	Status
No icon	Healthy/Operational
	Attention
	Degraded/Marginal
	Device Added
	Device Removed/Missing
	Down/Failed
	Routed In
	Routed Out
	Unknown/Link Down
	Virtual Switch

## Event Icons

For more information about events, refer to the *Event Management User Manual* or online help.

**TABLE 25** Event Icons

Icon	Description
	Informational
	Warning
	Fatal

# Keyboard Shortcuts

You can use the keystrokes shown in [Table 26](#) to perform common functions.

## NOTE

To open a menu using keystrokes, press **ALT** + the underlined letter. To open a submenu, release the **ALT** key first, then press the key for the underlined letter of the submenu option.

**TABLE 26** Keyboard Shortcuts

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse	CTRL + L
Command Tool	SHIFT + F4
Connectivity Map	F7
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Event Management	F11
Expand	CTRL + E
Help	F1
Insert Devices	CTRL +D
Internet Explorer	SHIFT + F1
Master Log	F5
Multiple Devices (Planned SAN only)	CTRL + D
Netscape	SHIFT + F2
New Plan	CTRL + N
Open Plan	CTRL + O
Open SAN menu	F10
Paste	CTRL + V
Product List	F9
Properties	CTRL + P
Security Center	F8
Select All	CTRL + A
Select Connections	CTRL + T
Show Ports	F4

**TABLE 26** Keyboard Shortcuts (Continued)

Menu Item or Function	Keyboard Shortcut
View Utilization	CTRL + U
Zoom In	CTRL + NumPad+
Zoom Out	CTRL + NumPad-

# Configuring EFCM Through a Firewall

---

## In this Appendix

This appendix provides optional procedures for configuring your SAN Management Client and Server applications to function across remote networks through a firewall.

- *Polling Client Function.....250*
- *Configuring TCP Port Numbers to Allow Firewall Access .....252*

## Polling Client Function

In some cases, a network may use virtual private network (VPN) or firewall technology, which can prohibit communication between a Server and the Client. In other words, a Client can find a Server, appear to log in, but is immediately logged out because the Server cannot reach the Client's remote object. To resolve this issue, the SAN Management application automatically detects the network configuration and runs the Client in "polling mode" when necessary.

When the Client is not running in polling mode, the Server calls the Client's remote object whenever it has new data. When the Client is running in polling mode, the Server queues up the data and the Client's remote object periodically (approximately every 5 or 10 seconds) checks in and gets the data. Thus, the original two-way communication is transformed into one-way communication, allowing passage through firewalls.

### Configuring for Faster Logins

When a Client attempts to log into a Server, the Server normally calls back to verify communication. In a firewall situation, this call fails and the Server automatically treats the Client as a "polling" Client. It may take up to 45 seconds for this call-back to fail (worst case). You can configure a polling parameter in configure properties files to let the Server know ahead of time that the Client is a "polling" Client. This skips the call-back from the Server and decreases the login time.

#### Forcing a Client to Be Polling

To force a specific Client to be a polling Client, edit the Client *config.properties* file located in the <Install\_Home>\resources\Client\ directory. Edit the *smp.callback.passive* parameter as in the following example.

This parameter only affects this Client; all other Clients can be regular Clients.

1. Open the <Install\_Home>\resources\Client\config.properties file using a text editor (for example, Notepad).
2. Go to the following lines:

```
# Forces this Client to be a polling Client.
# Enable by un-commenting this parameter.
# smp.callback.passive
```

3. Remove the pound sign (#) in front of the *smp.callback.passive* parameter.

```
# Forces this Client to be a polling Client.
# Enable by un-commenting this parameter.
smp.callback.passive
```

4. Save the file and restart the server.

## Forcing All Clients to Be Polling

To force all Clients communicating with a Server to be treated as polling Clients (regardless of the parameters the Clients launch with), edit the Server *config.properties* file located in the <Install\_Home>\resources\Server\ directory.

Edit the *smp.callback.passive* parameter as in the following example.

1. Open the <Install\_Home>\resources\Server\config.properties file using a text editor (for example, Notepad).

2. Go to the following lines:

```
# Force all Clients communicating with a Server to be treated as
# polling Clients (regardless of their startup parameters).
# Enable by un-commenting this parameter.
# smp.callback.passive
```

3. Remove the pound sign (#) in front of the *smp.callback.passive* line.

```
# Force all Clients communicating with a Server to be treated as
# polling Clients (regardless of their startup parameters).
# Enable by un-commenting this parameter.
smp.callback.passive
```

4. Save the file and restart the server.

## Configuring TCP Port Numbers to Allow Firewall Access

This section provides details about configuring TCP port numbers for RMI Servers and Registries to allow EFCM Client and Server application to function across firewalls.

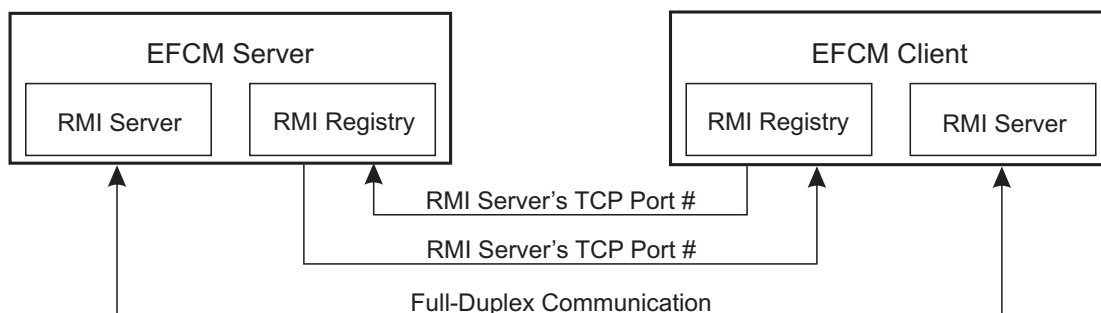
### EFCM with RMI at TCP Port Level

The RMI protocol lies between the EFCM application and the TCP/IP layer, as shown in the following table.

**TABLE 27** RMI Protocol Level

EFCM Server	EFCM Client
RMI	RMI
TCP/IP	TCP/IP

As shown in the following figure, the EFCM Server and Clients communicate with each other through the RMI Server. This is a full-duplex function. However, before the RMI Server on the EFCM Client can communicate with the RMI Server on the EFCM Server, it must know the TCP port number of the RMI Server. The function of the RMI registry is to communicate this TCP port number to the EFCM Client. Once this is done successfully, communication can take place between the RMI Server on the EFCM Server and the EFCM Client. (The EFCM Server obtains the TCP port number of the RMI Server on the Client during initial communications.)



**FIGURE 73** EFCM Server and Client Communications

The TCP port numbers of the RMI server are randomly and automatically selected on both the EFCM Server and Client as a full-duplex function. This poses a major problem for firewalls because the Client must be able to address the Server's RMI registry and the Server's remote objects. Also, the Server must be able to address the Client's remote objects. Firewalls are configured to block all unknown incoming connections with no mapping of outgoing connections based on a socket part of TCP and IP.

To work around this problem for EFCM, firewall administrators must set which ports are used by the Client and Server by editing parameters in EFCM M batch files. Use of the following procedures depend on how the firewall is set up. If the firewall prevents the Client from connecting to arbitrary ports on the Server, then you must fix both the Server's registry and export port. If the firewall prevents the Server from connecting to arbitrary ports on the Client, then you must fix the Client's export port.

- If the firewall prevents the Client from connecting to arbitrary ports on the Server, then perform both of these procedures:  
    [“Forcing Port in RMI Registry”](#) on page 253.  
    [“Forcing Server and Client Export Port Number”](#) on page 253.  
    **NOTE:** Configure the Server’s export port only.
- If the firewall prevents the Server from connecting to arbitrary ports on the Client, then configure the Client’s export port using the following procedure:  
    [“Forcing Server and Client Export Port Number”](#) on page 253.

## Forcing Port in RMI Registry

To force the RMI registry to use a particular TCP port for an RMI server, you must configure the Server Connection Port.

1. Select **SAN > Options**.  
    The **Options** dialog box displays.
2. In the **Category** list, select **Server Connection**.  
    The **Server Connection** fields display to the right of the **Category** list.
3. In the **Server Connection Port #** field, enter the TCP port number (between 0 - 65535).
4. Click **OK**.  
    **NOTE:** Changes to this option take effect after a application reboot.
5. Restart the application for your changes to take effect.

## Forcing Server and Client Export Port Number

To force the Server and Client to export a specific TCP port number for an RMI server, you must configure the client and the server export ports.

Note that the server and the client export ports are different ports. Although the server export number could match the client export port, it is not necessary.

1. Select **SAN > Options**.  
    The **Options** dialog box displays.
2. In the **Category** list, select **Client Export Port**.  
    The **Client Export Port** fields display to the right of the **Category** list.
3. In the **Client Export Port #** field, enter the TCP port number (number between 0 - 65535).
4. Click **Apply**.
5. In the **Category** list, select **Server Connection**.  
    The **Server Connection** fields display to the right of the **Category** list.

## D In this Appendix

6. In the **Server Export (SSL) Port #** field, enter the TCP port number.
7. Click **OK**.

**NOTE:** If the firewall prevents the Server from connecting to arbitrary ports on the Client, then you must force the export port of the Client. If the firewall prevents the Client from connecting to the Server, then just force the export port of the Server.

**NOTE:** Changes to this option take effect after a application reboot.

8. Restart the application for your changes to take effect.

# MySQL and DB2 Database Fields

---

## In this Appendix

This appendix provides reference information related to database exporting.

- *MySQL and DB2 Database Fields .....256*

## MySQL and DB2 Database Fields

When you export data to a MySQL or DB2 database, the information is displayed in database tables.

*ADAPTER Table*

*CONNECTION Table*

*DEVICE Table*

*FABRIC Table*

*HISTORICALPERFORMANCE Table*

*HOST Table*

*HOSTCONNECTION Table*

*HOSTHBAS Table*

*HOSTLUNS Table*

*IFCPLINK Table*

*LUN Table*

*LUNBINDING Table*

*LUNMASKING Table*

*MSAN Table*

*NETAPPFILER Table*

*PORT Table*

*REALTIMEPERFORMANCE Table*

*ROUTERFABRIC Table*

*SANROUTERSYSTEM Table*

*STORAGEDEVICES Table*

*ZONE Table*

*ZONELIBRARY Table*

*ZONEMEMBER Table*

*ZONEMEMBERDOMAINPORT Table*

*ZONEMEMBERFABRICADDRESS Table*

*ZONEMEMBERWWN Table*

*ZONESET Table*

*ZONESETZONES Table*

## ADAPTER Table

### NOTE

The Format table column displays values for both MySQL and DB2 databases. The values are the same for both databases, unless noted otherwise.

**TABLE 28**

Field	Definition	Format	Size
DEVICEGUID	Device GUID	Varchar	128
PWWN	Port world-wide name	Varchar	128
AVS	Vendor-specific ID	Varchar	128
ANSN	Node-symbolic name	Varchar	128
ADV	Driver version	Varchar	128
ASN	Serial number	Varchar	128
AORV	Option ROM version	Varchar	128
ANOP	Number of ports	Int	N/A
AFV	Firmware version	Varchar	128
ADN	Driver name	Varchar	128
ADES	Model description	Varchar	128
AMOD	Model	Char	128
AMF	Manufacturer	Char	128
AHV	Hardware version	Char	128
EXPORTTIME	Exported time	Varchar	128
Node Confidence	Node Confidence	Varchar	128
VirtualFabric ID	VirtualFabric ID	Int	11

## CONNECTION Table

**TABLE 29**

Field	Definition	Format	Size
SRCGUID	Source GUID	Varchar	128
SRCPORTNUMBER	Source port number	Int	N/A
TARGETGUID	Target GUID	Varchar	128
TARGETPORTNUMBER	Target port number	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## DEVICE Table

TABLE 30

Field	Definition	Format	Size
DEVICEGUID	Device GUID	Varchar	128
IBSTAT	Inband status	Varchar	128
NAME	Device name	Varchar	255
OBSTAT	Out-of-band status	Varchar	128
DEVICETYPE	Type of device	Varchar	128
PORTCOUNT	Number of ports on device	Int	N/A
PORTNAME	Port name of device	Varchar	255
SERIALNUMBER	Serial number of device	Varchar	255
VENDOR	Manufacturer	Varchar	128
MODEL	Model of device	Varchar	128
IPADDRESS	IP address number	Varchar	128
FCADDRESS	Fibre Channel address	Varchar	128
WWN	World-wide name	Varchar	128
FIRMWARE	Firmware version	Varchar	128
DEVICEAVAILABLE	Is device available?	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## FABRIC Table

TABLE 31

Field	Definition	Format	Size
NAME	Fabric Name	Varchar	128
Nickname	Fabric nickname	Varchar	128
EXPORTTIME	Exported time	Varchar	128

## HISTORICALPERFORMANCE Table

**TABLE 32**

Field	Definition	Format	Size
STARTTIME	Start time	Varchar	128
DEVICEGUID	Device GUID	Varchar	128
PORTNUMBER	Port number	Int	N/A
TYPE	Type of performance (i.e. day, hr)	Varchar	128
BIN	Bin number	Int	N/A
TX	Transmit	Int	N/A
RX	Receive	Int	N/A
CRC	Invalid CRC count	Int	N/A
LOS	Loss of signal	Int	N/A
OOS	Out of sync	Int	N/A
MBW	Max bandwidth	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## HOST Table

**TABLE 33**

Field	Definition	Format	Size
ID	Host ID	MySQL: Int unsigned DB2: Int	11
NICKNAME	Nickname of the host	Varchar	255
HOSTNAME	Name of the host	Varchar	128
IPADDRESS	IP address number	Varchar	128
OS	Operating System	Varchar	128
ASSIGNEDLUNS	Assigned LUNs	Int	11
TOTALSIZE	Total size of the host	MySQL: Float DB2: Double	N/A
APPLICATIONS	Host applications	Varchar	255
DEPARTMENT	Department of the host	Varchar	128
LOCATION	Location of the host	Varchar	128
CONTACT	Contact information of the host	Varchar	255

**TABLE 33**

Field	Definition	Format	Size
DESCRIPTION	Host description	Varchar	255
COMMENTS	Comments	Varchar	255
EXPORTTIME	Exported time	Varchar	128

## HOSTCONNECTION Table

**TABLE 34**

Field	Definition	Format	Size
DEVICEGUID	Storage device GUID	Varchar	255
NICKNAME	Nickname	Varchar	255
HBANWWN	HBA Node World Wide Name	Varchar	128
HBAPWWN	HBA Port WWN	Varchar	128
OSNAME	Operating System Profile Name	Varchar	128
STORAGENWWN	Storage Node WWN; could be empty if this host is permitted to access all ports	Varchar	128
STORAGEPWWN	Storage Port WWN; could be empty if this host is allowed to access all ports	Varchar	128
CABLED	Whether Fibre Channel connection exists between the host port and this storage port	Int	N/A
ZONED	Whether the host port and the storage port are zoned together	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## HOSTHBAS Table

**TABLE 35**

Field	Definition	Format	Size
HOSTID	ID of the host containing the HBA	MySQL: Int unsigned DB2: Int	N/A
HBADeviceGUID	DEVICEGUID of the contained HBA	Varchar	128
EXPORTTIME	Exported time	Varchar	128

## HOSTLUNS Table

**TABLE 36**

Field	Definition	Format	Size
PORTGUID	Port GUID	Varchar	255
LUNGUID	LUN GUID	Varchar	255
TARGETPORTGUID	Target Port GUID	Varchar	255
ID	Host size LUN ID (HLU)	Int	N/A
BUSID	Bus ID of the LUN	Int	N/A
TARGETID	Target ID of the LUN	Int	N/A
LATENCY	SCSI inquiry time for the LUN	Int	N/A
OSDEVICENAME	OSDeviceName of the LUN	Varchar	255
VOLUME	Volume Name of the LUN	Varchar	255
VOLUMELABEL	Volume Label of the LUN	Varchar	255
MOUNTPATH	Mount Path of the LUN	Varchar	128
EXPORTTIME	Exported time	Varchar	128

## IFCPLINK Table

**TABLE 37**

Field	Definition	Format	Size
IFCPLINKID	ID of iFCP link	Varchar	255
SANROUTERWWN	WWN of the SAN Router	Varchar	255
LOCALIP	Local IP Address of the SAN Router	Varchar	255
REMOTEIP	Remote IP Address of the SAN Router	Varchar	255
LOCALPORT	Local port number of the SAN Router	Int	11
REMOTEPORT	Remote port number of the SAN Router	Int	11
STATUS	Status of the SAN Router	Varchar	255
EXPORTTIME	Exported time	Varchar	128

## LUN Table

**TABLE 38**

Field	Definition	Format	Size
LUNGUID	LUN GUID	Varchar	255
DEVICEGUID	Device GUID to which the LUN belongs	Varchar	255
NAME	LUN name	Varchar	255
ID	Internal LUN ID (ALU)	Int	N/A
UNIQUEID	Unique ID	Varchar	255
ASSIGNED	Masked, Bound, Unbound	Varchar	128
STATE	Normal, Transitioning, Faulted, Expanding, Defragmenting	Varchar	128
HOTSPARES	Number of hot spares in the LUN	Int	N/A
RAIDTYPE	RAID type of the LUN	Varchar	128
TOTALSIZE	Total LUN size in GB	MySQL: Float DB2: Double	4
BLOCKSIZE	Block size in B	Int	N/A
DISKCOUNT	Number of disks the LUN is striped across	Int	N/A
EXPORTTIME	Exported time of the data	Varchar	128

## LUNBINDING Table

**TABLE 39**

Field	Definition	Format	Size
LUNGUID	LUN GUID	Varchar	255
NWWN	Node World Wide Name; could be empty if LUN is bound to all ports	Varchar	128
PWWN	Port World Wide Name; is ALL if LUN is bound to all ports	Varchar	128
HOSTMODE	Host Mode; meaningful only for HDS	Varchar	128
LUNID	ID used in binding LUN to this port	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## LUNMASKING Table

**TABLE 40**

Field	Definition	Format	Size
LUNGUID	LUN GUID	Varchar	255
HBANWWN	HBA Node World Wide Name	Varchar	128
HBAPWWN	HBA Port World Wide Name	Varchar	128
STORAGENWWN	Storage port node World Wide Name; could be empty if masking is not restricted to any storage ports	Varchar	128
STORAGEPWWN	Storage port World Wide Name; could be empty if masking is not restricted through any port	Varchar	128
CABLED	Whether Fibre Channel connection exists between the host port and this storage port	Int	N/A
ZONED	Whether the host port and the storage port are zoned together	Int	N/A
EXPORTTIME	Exported time	Varchar	128

## MSAN Table

**TABLE 41**

Field	Definition	Format	Size
NAME	Name of the mSAN	Varchar	20
SANID	ID of the mSAN	Varchar	255
NICKNAME	Nickname of the mSAN	Bigint	255
ROUTERFABRICCOUNT	SAN Router fabric count of the mSAN	Int	11
FCFABRICCOUNT	Fibre Channel fabric count of the mSAN	Int	11
EXPORTTIME	Exported time	Varchar	128

## NETAPPFILER Table

**TABLE 42**

Field	Definition	Format	Size
WWN	WWN of the NetApp Filer	Varchar	255
INTERSYSTEMLINKCOUNT	Intersystem link count of the NetApp Filer	Int	11
ISCLUSTER	IS Cluster of the NetApp Filer	Varchar	255
EXPORTTIME	Exported time	Varchar	128

## PORT Table

**TABLE 43**

Field	Definition	Format	Size
DEVICEGUID	Device GUID	Varchar	128
PWWN	Port world-wide name	Varchar	128
PORTNUMBER	Port number	Int	11
FABRICNAME	Fabric name	Varchar	128
FABRICADDRESS	Address of the fabric to which the port belongs	Varchar	128
TYPE	Port type	Varchar	128
STATE	Port state	Varchar	128
SUPPORTEDCOS	Class of Service (COS) supported by the port	Varchar	128
SUPPORTEDFC4TYPE	FC4 type supported by the port	Varchar	128
SYMBOLICNAME	Symbolic Name of the port	Varchar	128
OSDEVICENAME	OS Device Name of the port	Varchar	128
SPEED	Port speed	Varchar	128
SUPPORTEDSPEED	Speed supported by the port	Varchar	128
MAXFRAMESIZE	Maximum frame size supported by the port	Varchar	128
VLANENABLED	VLAN enabled	Varchar	128
VLANID	ID of the VLAN	Int	11
L2COS	L2 Class of Service	Int	11
MTUSIZE	MTU size	Int	11
ExportTime	Exported time	Varchar	128

## REALTIMEPERFORMANCE Table

**TABLE 44**

Field	Definition	Format	Size
DEVICEGUID	Device GUID	Varchar	128
PORTNUMBER	Port number	Int	N/A
TX	Transmit	Int	N/A
RX	Receive	Int	N/A
CRC	Invalid CRC count	Int	N/A
LOS	Loss of signal	Int	N/A
OOS	Out of sync	Int	N/A
MBW	Max bandwidth	Int	N/A
TSTAMP	Time stamp	Varchar	128
PS_ITXW	Invalid Transmitted Words	Number	N/A
PS_ICRC	Number of frames received with invalid CRC	Number	N/A
PS_TIM	Time Stamp	Number	N/A

## ROUTERFABRIC Table

**TABLE 45**

Field	Definition	Format	Size
NAME	Name of the SAN Router fabric	Varchar	255
ID	ID of the SAN Router fabric	Bigint	20
CLUSTERID	Cluster ID of the SAN Router fabric	Int	11
NICKNAME	Nickname of the SAN Router fabric	Varchar	255
IFCP LINKCOUNT	iFCP link count of the SAN Router fabric	Int	11
EXPORTTIME	Exported time	Varchar	128
FCHALinkCount	FCHA Link Count	Int	11

## SANROUTERSYSTEM Table

**TABLE 46**

Field	Definition	Format	Size
IPADDRESS	IP Address of the SAN Router system	Varchar	255
NODEWWN	Node WWN of the SAN Router system	Varchar	255
NICKNAME	Nickname of the SAN Router system	Varchar	255
PORTCOUNT	Port count of the SAN Router system	Int	11
IFCPSANID	iFCP SAN ID of the SAN Router system	Bigint	11
CLUSTERID	Cluster ID of the SAN Router system	Int	11
VENDOR	Vendor of the SAN Router system	Varchar	255
MODEL	Model of the SAN Router system	Varchar	255
FIRMWARE	Firmware of the SAN Router system	Varchar	255
FCHALINKCOUNT	iFCP link count of the SAN Router system	Int	11
IFCPLINKCOUNT	iFCP link count of the SAN Router system	Int	11
DNSNAME	DNS name of the SAN Router system	Varchar	255
LOCATION	Location of the SAN Router system	Varchar	255
CONTACT	Contact name of the SAN Router system	Varchar	255
EXPORTTIME	Exported time	Varchar	128

## STORAGEDEVICES Table

### NOTE

The storage devices table is only populated with information about the storage devices when the server is able to discover the LUNs on the storage. The server must have the LUN Management license and the storage device must be discovered using a specialized mechanism, such as API's or CLI's. LUN Management is an optional module available to previous LUN Management licensed customers.

**TABLE 47**

Field	Definition	Format	Size
DEVICEGUID	Storage device GUID	Varchar	255
NAME	Storage device name	Varchar	255
MODEL	Model name	Varchar	255
VENDOR	Vendor name	Varchar	255
TOTALSIZE	Total size of the device	MySQL: Float DB2: Double	N/A
FREESPACE	Free space available on the device	MySQL: Float DB2: Double	N/A
FREESPACECOUNT	Number of Free spaces available on the device	Int	N/A
ASSIGNEDLUNSPACE	Total Size of the LUNs assigned	MySQL: Float DB2: Double	N/A
ASSIGNEDLUNCOUNT	Total number of LUNs assigned	Int	N/A
FREELUNSPACE	Total Size of all the LUNs which have not been assigned	MySQL: Float DB2: Double	N/A
FREELUNCOUNT	Total number of LUNs which have not been assigned	Int	N/A
ASSIGNEDHOSTSCOUNT	Total number of hosts which have been assigned	Int	N/A
EXPORTTIME	Exported time of the data	Varchar	128

## ZONE Table

**TABLE 48**

Field	Definition	Format	Size
ID	Zone set ID	Varchar	255
ZONELIBRARYID	ID of zone library the zone set belongs to	Varchar	255
NAME	Name of the zone set	Varchar	255
MINGUARANTEEDBANDWIDTH	Minimum guaranteed bandwidth	Int	11

**TABLE 48**

Field	Definition	Format	Size
MAXALLOWEDBANDWIDTH	Maximum allowed bandwidth	Int	11
ISISNSIMPORTED	iSNS imported	Varchar	128
EXPORTTIME	Exported time of the data	Varchar	128

## ZONELIBRARY Table

**TABLE 49**

Field	Definition	Format	Size
ID	Library ID	Varchar	255
FABRICNAME	Name of the fabric the library belongs to	Varchar	128
TYPE	'Discovered' or 'name of SAN Management application'	Varchar	128
ACTIVEZONESETID	ID of the active zone set, if any	Varchar	255
EXPORTTIME	Exported time of the data	Varchar	128

## ZONEMEMBER Table

**TABLE 50**

Field	Definition	Format	Size
ID	Zone member ID	MySQL: Int unsigned DB2: Int	N/A
ZONEID	ID of the zone the member belongs to	Varchar	255
MEMBERTYPE	Type of the member (WWN, Domain/Port, FabricAddress)	Varchar	128
EXPORTTIME	Exported time of the data	Varchar	128

## ZONEMEMBERDOMAINPORT Table

**TABLE 51**

Field	Definition	Format	Size
ID	ID of the member in the ZoneMember table	MySQL: Int unsigned DB2: Int	N/A
DOMAIN	Domain	MySQL: Smallint unsigned DB2: Smallint	N/A
PORT	Port	MySQL: Smallint unsigned DB2: Smallint	N/A
EXPORTTIME	Exported time of the data	Varchar	128

## ZONEMEMBERFABRICADDRESS Table

**TABLE 52**

Field	Definition	Format	Size
ID	ID of member in the ZoneMember table	MySQL: Int unsigned DB2: Int	N/A
FABRICADDRESS	Fabric address	Varchar	128
EXPORTTIME	Exported time of the data	Varchar	128

## ZONEMEMBERWWN Table

**TABLE 53**

Field	Definition	Format	Size
ID	ID of the member in the ZoneMember table	Int	11
WWN	World wide name	Varchar	128
EXPORTTIME	Exported time of the data	Varchar	128

## ZONESET Table

**TABLE 54**

Field	Definition	Format	Size
ID	Zone set ID	Varchar	255
ZONELIBRARYID	ID of zone library the zone set belongs to	Varchar	255
NAME	Name of the zone set	Varchar	255
ISACTIVE	Active	Varchar	128
ExportTime	Exported time of the data	Varchar	128

## ZONESETZONES Table

**TABLE 55**

Field	Definition	Format	Size
ZONESETID	ID of the zone set	Varchar	255
ZONEID	ID of the zone	Varchar	255
IFCPLINKID	ID of the iFCP link	Varchar	255
ExportTime	Exported time of the data	Varchar	128

# User Privileges

---

## In this Appendix

EFCM provides the User Administrator with a high level of control over what functions your users can see and/or use. This section describes the effect that each user privilege has on the application when placed in one of the three available configurations: no privilege, read-only, and read/write.

User privilege is EFCM's method of providing roll-based access control (RBAC) to the software's user administrator.

This appendix provides information about user privileges and access levels.

- *About User Privileges* .....272
- *About User Groups and Access Levels* .....285

## About User Privileges

In EFCM groups are assigned privileges and views. Privileges are not directly assigned to users; users get privileges because they belong to groups. If a user is assigned to two or more groups they receive the highest level (no privilege, read-only, read/write) for the privilege assigned to any of the groups to which they belong. The following table defines all the privileges in EFCM and the behavior of the application if the privilege is not given, read only, or read/write.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Active Session Management	Allows you to view and disconnect client sessions.	Disables the <b>Active Sessions</b> command on the <b>SAN</b> menu.	Enables the <b>Active Sessions</b> command on the <b>SAN</b> menu. Allows you to open the <b>Active Sessions</b> dialog box; however, disables the <b>Disconnect User</b> and <b>OK</b> buttons.	Enables the <b>Active Sessions</b> command on the <b>SAN</b> menu. Enables all functions in the <b>Active Sessions</b> dialog box.
Add/Delete Properties	Allows you to define new properties as well as remove them.	Disables the <b>Add</b> , <b>Edit</b> and <b>Delete</b> buttons on the <b>Create View</b> dialog box <b>Columns</b> tab. Disables the <b>Add Column</b> , <b>Edit Column</b> , and <b>Delete Column</b> commands on the right-click menu of the <b>Product List</b> column headers. Disables the <b>Add</b> , <b>Edit</b> , and <b>Delete</b> commands on the property headers in property sheets.	Same as No Privilege	Enables the <b>Add</b> , <b>Edit</b> , and <b>Delete</b> properties commands and buttons in the <b>Create View</b> and <b>Edit View</b> dialog boxes, the <b>Product List</b> column header right-click menu, and the Property Sheet property header right-click menu.
Advanced Call Home	Allows you to configure call home centers, devices, and event filters.	Disables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu.	Enables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu; however, disables the <b>Add</b> , <b>Edit</b> , <b>Remove</b> , <b>Edit</b> Centers, <b>Add/Remove Centers</b> , <b>OK</b> , and <b>Apply</b> buttons, as well as the <b>Enabled</b> check boxes.	Enables the <b>Advanced Call Home</b> command on the <b>Monitor &gt; Event Notification</b> menu. Enables all functions in the dialog box.
Backup	Allows you to control the function that copies (backs up) the application data files to another disk.	Disables the <b>Backup Now</b> and <b>Configure</b> commands on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the <b>Options</b> dialog box.	Disables the <b>Configure</b> command on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the <b>Options</b> dialog box.	Enables the <b>Backup Now</b> and <b>Configure</b> commands on the Backup icon right-click menu on the application status bar. Enables all functions for Backup on the <b>Options</b> dialog box.
Discover On/Off	Allows you to turn product discovery on and off.	Disables the <b>On</b> and <b>Off</b> commands in the <b>Discover</b> menu.	Same as No Privilege	Enables the <b>On</b> and <b>Off</b> commands in the <b>Discover</b> menu.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Discovery Setup	Allows you to configure discovery setup.	Disables <b>Setup</b> on the <b>Discover</b> menu and toolbar.	Enables <b>Setup</b> on the <b>Discover</b> menu and toolbar. Allows you to open the <b>Discovery Setup</b> dialog box; however, disables the <b>OK</b> button.	Enables <b>Setup</b> on the <b>Discover</b> menu and toolbar. Enables all functions in the <b>Discovery Setup</b> dialog box.
E-mail Event Notification Setup	Allows you to define the e-mail server used to send e-mail.	Disables <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Currently asks, "Are you sure you want to assign Event Management privileges to this group that does not otherwise have read/write for: E-mail Event Notification Setup?".	Enables the <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Allows you to open the <b>E-Mail Event Notification Setup</b> dialog box; however, disables the <b>OK</b> button.	Enables <b>Event Notification E-mail</b> command on the <b>Monitor</b> menu and the <b>E-mail Event Notification Setup</b> button in the <b>Users</b> dialog box. Enables all functions in the <b>E-Mail Event Notification Setup</b> dialog box.
Enterprise Fabric Mode	Allows you to activate Fabric Binding, Switch Binding, Insistent Domain ID, and Domain RSCN's.	Disables the <b>Enterprise Fabric Mode</b> command from <b>Configure</b> menu.	Allows you to open the <b>Enterprise Fabric Mode</b> dialog box; however, disables the <b>OK</b> button.	Enables <b>Enterprise Fabric Mode</b> command from <b>Configure</b> menu. Enables all functions in the <b>Enterprise Fabric Mode</b> dialog box.
Event Management	Allows you to define rules with event triggers and actions.	Disables the <b>Event Management</b> tab.	Enables access to the <b>Event Management</b> tab and allows existing rules to be selected and viewed. Disables all action buttons on the tab.	Enables access to the <b>Event Management</b> tab and enables all functions on the tab.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Export	Allows you to export SAN files, Performance data, Master logs, Connectivity map, Connectivity XML, Product list, Reports, Nicknames, Status, and Zone set activation history.	Disables the <b>Export</b> command on the <b>SAN</b> menu. Disables the Master Log right-click <b>Export</b> command. If this privilege is removed and the Event Management privilege is assigned then give this message: <title: <Product> Message> <Warning>Removing the Export privilege does not remove users' ability Export in Event Management. You might also want to consider removing the Event Management privilege as well. <<OK>>	Enables the <b>Export</b> command on the <b>SAN</b> menu. Allows you to open the <b>Export Discovered SAN</b> dialog box; however, disables the <b>OK</b> and <b>Apply</b> buttons.	Enables the <b>Export</b> command on the <b>SAN</b> menu. Enables all functions in the <b>Export Discovered SAN</b> dialog box.
Fabric Binding	Allows you to define the switches allowed to join a fabric. Allows you to control access to the <b>Fabric Binding</b> dialog box from the <b>Configure</b> menu.	Disables the <b>Fabric Binding</b> command on the <b>Configure</b> menu.	Enables the <b>Fabric Binding</b> command on the <b>Configure</b> menu; however, disables the <b>OK</b> button.	Enables the <b>Fabric Binding</b> command on the <b>Configure</b> menu. Enables all functions in the dialog box.
Frame Sniffer	Allows you to count frames passed by a switch port that meet specific criteria. Allows you to control access to the <b>Frame Sniffer</b> dialog box from the <b>Monitor</b> menu.	Disables the <b>Frame Sniffer</b> command on the <b>Monitor</b> menu.	Enables the <b>Frame Sniffer</b> command on the <b>Monitor</b> menu; however, disables the <b>OK</b> button.	Enables the <b>Frame Sniffer</b> command on the <b>Monitor</b> menu. Enables all functions in the dialog box.
Group Manager – Create Event Log	Allows you to create a log that lists all events that are associated with any of the products in the specified group. Allows you to control access to the <b>Create Event Log</b> function.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu; however, disables the <b>Create Event Log</b> option. Disables <b>Log &gt; Group</b> on the <b>Monitor</b> menu.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu; however, disables the <b>Create Event Log</b> option. Enables <b>Group Log</b> on the <b>Monitor</b> menu.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu and enables the <b>Create Event Log</b> option. Enables <b>Group Log</b> on the <b>Monitor</b> menu.
Group Manager – Firmware Install	Allows you to install firmware on a group of products (either switches or directors). Allows you to control access to the <b>Firmware Install</b> function.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu; however, disables the <b>Firmware Install</b> option.	Same as no privilege.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu and enables the <b>Firmware Install</b> option.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Group Manager – Run Data Collection	Allows you to collect maintenance data about a group of switches or directors. Allows you to control access to the <b>Run Data Collection</b> function.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu; however, disables the <b>Run Data Collection</b> option.	Same as no privilege.	Enables the <b>Group Manager</b> command on the <b>Configure</b> menu and enables <b>Run Data Collection</b> option.
Import	Allows you to import SAN files (zip), SANvergence Manager Data (mSAN list), Nicknames, Properties (csv) of products and ports, Server HBA Mappings (csv), Storage Port Mappings (csv), Zone set activation history (zip), and FC Aliases into Nicknames. Allows you to control access to the <b>Import</b> dialog box from <b>SAN</b> menu.	Disables the <b>Import</b> command on the <b>SAN</b> menu.	Same as no privilege.	Enables the <b>Import</b> command on the <b>SAN</b> menu and enables the functions in the dialog box.
License Update	Allows you to update your license. Allows you to control access to the <b>License</b> dialog box from the <b>Help</b> menu.	Disables the <b>License</b> command on the <b>Help</b> menu.	Enables the <b>License</b> command on the <b>Help</b> menu; however, disables the <b>Update</b> and <b>OK</b> buttons.	Enables the <b>License</b> command on the <b>Help</b> menu and enables you to change the license key.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Log Management	Allows you to control access to the Export, <b>Clear</b> , <b>Show</b> and <b>Hide</b> commands in the Master Log and individual logs (audit, event, fabric, group, product status, session, and security).	Disables the <b>Export</b> , <b>Clear</b> , <b>Show</b> and <b>Hide</b> commands in the Master Log and individual logs. Enables <b>Show All</b> and <b>Export</b> commands. Disables the <b>Clear</b> and <b>Export</b> buttons on the individual logs. Note that the <b>Export</b> command on the master log right-click menu is controlled by the Export privilege (launches the <b>Export Discovered SAN</b> dialog box). If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>Removing the Log Management privilege does not remove users' ability for Log Management in Event Management. You might also want to consider removing the Event Management privilege as well. <<OK>>	Same as No Privilege	Enables the <b>Export</b> , <b>Clear</b> , <b>Show</b> , and <b>Hide</b> commands for the master log and individual logs. Enables the commands on the master log right-click menu (except possibly the <b>Export</b> command). Note that the <b>Export</b> command on the master log is dependent on both this privilege and the Export privilege because this command opens the <b>Export Discovered SAN</b> dialog box. Enables all functions in the individual logs.
Map Editing	Recommend Remove			
Map Loop to Hub	Allows you to identify the discovered hub that is replacing or can replace a loop icon in the Connectivity Map.	Disables the <b>Map to Hub</b> command in the <b>Discover</b> menu and on loop icons.	Same as No Privilege	Enables all <b>Map to Hub</b> functions.
Map Port to Storage	Allows you to construct multi-port storage systems out of individual storage ports.	Disables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu and right-click menus for Storage products and ports in the tree and map.	Enables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu right-click menus for Storage products and ports in the tree and map. Allows you to open the <b>Storage Port Mapping</b> dialog box; however, disables the <b>Create</b> , <b>Delete</b> , right and left arrow, and <b>OK</b> buttons.	Enables the <b>Storage Port Mapping</b> command from <b>Discover</b> menu and right-click menus for Storage products and ports in the tree and map. Enables all functions on the <b>Storage Port Mapping</b> dialog box.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Monitor Ethernet Event	Allows you to enable events for loss of Ethernet connection.	Disables <b>Ethernet Event</b> on the <b>Monitor</b> menu.	Enables <b>Ethernet Event</b> on the <b>Monitor</b> menu. Allows you to open the <b>Configure Ethernet Event</b> dialog box; however, disables the <b>Enable Ethernet</b> check box, the <b>Ethernet Timeout</b> text box, and the <b>OK</b> button.	Enables <b>Ethernet Event</b> on the <b>Monitor</b> menu. Enables all functions on the <b>Configure Ethernet Event</b> dialog box.
Performance	Allows you to configure the performance subsystem, the display of performance graphs, and threshold settings.	Disables entire <b>Performance</b> submenu off the <b>Monitor</b> menu as well as the right-click <b>Performance Graph(s)</b> command on ports and switch products.	Enables entire <b>Performance</b> submenu off the <b>Monitor</b> menu as well as the right-click <b>Performance Graph(s)</b> command on ports and switch products. Allows you to open the <b>Performance Setup</b> dialog box; however, disables the <b>OK</b> button. No changes can be made. Allows you to open the <b>Performance Graphs</b> dialog box and enables all controls; however, disables the check boxes under the <b>Set Thresholds</b> label on the individual port dialog box (double-click a graph).	Enables entire <b>Performance</b> submenu off the <b>Monitor</b> menu and the right-click <b>Performance Graph(s)</b> command on ports and switch products. Enables changes to the <b>Performance Setup</b> dialog box. Allows you to open the <b>Performance Graphs</b> dialog box and enables all controls. Enables all functions on the individual port dialog box (double-click a graph).
Persist Fabric	Allows you to define the current devices and connections present in a fabric as a baseline and to highlight any changes to that baseline	Disables the <b>Persist Fabric</b> , <b>Unpersist Fabric</b> , and <b>Unpersist Product</b> commands on the <b>Monitor</b> menu and right-click menus of Fabrics and Products. Allows you to see the persistence displays.	Same as no privilege.	Enables the <b>Persist Fabric</b> , <b>Unpersist Fabric</b> , and <b>Unpersist Product</b> commands on the <b>Monitor</b> menu and right-click menus of Fabrics and Products.
Planning	Allows you to display and edit a planning desktop.	Disables the <b>Planned SAN</b> button on the main toolbar, the <b>New</b> , <b>Open</b> , <b>Save</b> , and <b>Save As Plan</b> commands in the <b>SAN</b> menu and the <b>Planned SAN</b> command on the <b>View</b> menu.	Enables the <b>Open Plan</b> command in the <b>SAN</b> menu which allows you to display a SAN Plan.	Enables the <b>Planned SAN</b> button on the main toolbar and the <b>New</b> , <b>Open</b> , <b>Save</b> , and <b>Save As Plan</b> commands in the <b>SAN</b> menu and the <b>Planned SAN</b> command on the <b>View</b> menu.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Port Fencing	Allows you to configure the function that logs ports out of fabrics automatically if they are misbehaving.	Disables the <b>Port Fencing</b> command from the <b>Configure</b> menu.	Enables the <b>Port Fencing</b> command from the <b>Configure</b> menu. Disables the Thresholds <b>Add</b> , <b>Edit</b> , and <b>Delete</b> buttons, the right- and left-arrow threshold assignment buttons, and the <b>Port Unblock</b> and <b>Properties</b> buttons, and the <b>OK</b> button on the <b>Port Fencing</b> dialog box.	Enables the <b>Port Fencing</b> command from the <b>Configure</b> menu. Enables all functions on the <b>Port Fencing</b> dialog box.
Product Administration <b>NOTE:</b> This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables most functionally.	Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights. Displays the message, "You do not have rights to perform this action."	Same as No Privilege	Enables the functions described in the <i>Element Manager User Manual</i> .
Product Maintenance <b>NOTE:</b> This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables maintenance functions.	Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights. Displays the message, "You do not have rights to perform this action."	Same as No Privilege	Enables the functions described in the <i>Element Manager User Manual</i> .
Product Operation <b>NOTE:</b> This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables operator functions.	Disables the functions described in the <i>Element Manager User Manual</i> for which you do not have rights. Displays the message, "You do not have rights to perform this action."	Same as No Privilege	Enables the functions described in the <i>Element Manager User Manual</i> .
Properties Edit	Allows you to edit many director and switch properties.	Enables the <b>Properties</b> command on <b>Edit</b> menu and right-click menus. Disables edit function (removes green triangles) from editable property fields.	Same as No Privilege	Enables <b>Properties</b> command on <b>Edit</b> menu and right-click menus. Enables editable properties (marked by a green triangle) in the Product List and the Properties Sheets.
Remote Access	Allows you to limit access of clients coming from specific IP addresses.	Disables the <b>Remote Access</b> command on the <b>SAN</b> menu.	Enables the <b>Remote Access</b> command on the <b>SAN</b> menu. Allows you to open the <b>Remote Access</b> dialog box; however, disables the <b>OK</b> button.	Enables the <b>Remote Access</b> command on the <b>SAN</b> menu. Enables all functions on the <b>Remote Access</b> dialog box.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Report	<p>Allows you to generate and view the following reports:</p> <ul style="list-style-type: none"> <li>Consistency</li> <li>iFCP Connections and Zones</li> <li>LUN Mapping</li> <li>Name Server,</li> <li>R Port</li> <li>Router configuration,</li> <li>Zone Library reports.</li> </ul>	<p>Disables the <b>Reports &gt; View</b> command and the <b>Reports &gt; Generate</b> command on the <b>Monitor</b> menu.</p> <p>If this privilege is removed and the Event Management privilege is assigned then this message appears:</p> <p>&lt;title: &lt;Product&gt; Message&gt;</p> <p>&lt;Warning&gt;Removing the Report privilege does not remove users' ability to generate reports in Event Management. You might also want to consider removing the Event Management privilege as well.</p> <p>&lt;&lt;OK&gt;&gt;</p>	<p>Enables the <b>Reports &gt; View</b> command on the <b>Monitor</b> menu.</p> <p>Disables the <b>Reports &gt; Generate</b> command on the <b>Monitor</b> menu.</p>	<p>Enables the <b>Reports &gt; View</b> command and the <b>Reports &gt; Generate</b> command on the <b>Monitor</b> menu.</p>
Security Admin	Allows you to enable and configure SANtegrity features.	<p>Disables the <b>Security</b> tab.</p> <p>Disables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> and the <b>Security Center</b> command in the <b>View &gt; Show Panels</b> menu.</p>	<p>Enables the <b>Security</b> tab.</p> <p>Enables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> and the <b>Security Center</b> command in the <b>View &gt; Show Panels</b> menu; however, disables all functional buttons in the <b>Users, Software, Devices, IP Access Control, and Radius Servers</b> tabs in the <b>Security Center</b>. Disables the <b>Clear</b> button the <b>Security Log</b> dialog box.</p> <p>Enables the <b>Export</b> button in the <b>Security Log</b> dialog box.</p>	<p>Enables the <b>Security</b> tab.</p> <p>Enables the <b>Security Log</b> command on the <b>Monitor &gt; Logs</b> and the <b>Security Center</b> command in the <b>View &gt; Show Panels</b> menu. Enables all functions in the <b>Security Center</b>.</p> <p>Enables all functions in the <b>Security Log</b> dialog box.</p>
Servers	Allows you to identify all the HBAs that are in the same server.	<p>Disables the <b>Servers</b> command from the <b>Discover</b> menu.</p> <p>Disables the <b>Server</b> right-click command on HBAs.</p>	<p>Enables <b>Servers</b> command from the <b>Discover</b> menu and right-click menu; however, disables the <b>Create, Delete, and OK</b> buttons.</p>	<p>Enables <b>Servers</b> command from the <b>Discover</b> menu and right-click menu.</p> <p>Enables all functions in the <b>Servers</b> dialog box.</p>

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Setup Tools	Allows you to define and place commands on product icons and in the <b>Tools</b> menu.	Disables the <b>Setup Tools</b> command on the <b>Tools</b> menu. Any existing <b>Tools</b> and/or right-click commands already defined or defined by others are available for use; however, you cannot configure new items. If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>Removing the Log Management privilege does not remove users' ability for Setup Tools in Event Management. You might also want to consider removing the Event Management privilege as well. <<OK>>	Enables the <b>Setup Tools</b> command on the <b>Tools</b> menu; however, disables the <b>OK</b> button.	Enables the <b>Setup Tools</b> command on the <b>Tools</b> menu. Enables all functions in the <b>Setup Tools</b> dialog box.
Show Route	Allows you to highlight the route through the fabric that two-end nodes use to communicate.	Disables the <b>Show Route</b> commands on the <b>Monitor</b> menu and right-click menus on ports. Disables the <b>Hide Route</b> command on the <b>Monitor</b> menu.	Same as no privilege.	Enables the <b>Show Route</b> commands on the <b>Monitor</b> menu and right-click menus on ports.
Shutdown	Allows you to exit and close the server and optionally the client.	Disables the <b>Shutdown</b> command on the <b>SAN</b> menu.	Same as no privilege.	Enables the <b>Shutdown</b> command on the <b>SAN</b> menu.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
SNMP Agent Configuration	Allows you to configure community strings and trap recipients for the SNMP Agent.	Disables the <b>SNMP Agent &gt; On, Off, and Setup</b> commands on the <b>Monitor</b> menu. If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>Removing the SNMP privilege does not remove users' ability for SNMP configuration in Event Management. You might also want to consider removing the Event Management privilege as well. <<OK>>	Disables the <b>SNMP Agent &gt; On</b> and <b>Off</b> commands on the <b>Monitor</b> menu. Enables the <b>SNMP Agent &gt; Setup</b> command on the <b>Monitor</b> menu; however, disables all functions in the <b>SNMP Setup</b> dialog box.	Enables the <b>SNMP Agent &gt; On, Off, and Setup</b> commands on the <b>Monitor</b> menu. Enables all functions in the <b>SNMP Setup</b> dialog box.
Software Configuration Parameters	Allows you to configure some of the properties of the client and server of the management application.	Disables the <b>Software Configuration Parameters</b> folder and sub pages in the <b>Options</b> dialog box. The configuration cannot be viewed.	Enables the <b>Software Configuration Parameters</b> folder and sub pages in the <b>Options</b> dialog box; however, disables the <b>OK</b> and <b>Apply</b> buttons when any of the sub pages are selected.	Enables the <b>Software Configuration Parameters</b> folder and sub pages in the <b>Options</b> dialog box. Enables all functions when any of those sub pages are selected.
Trap Forwarding	Allows you to specify where to forward the traps it receives from other systems.	Disables the <b>Trap Forwarding</b> command from the <b>Monitor</b> menu.	Enables the <b>Trap Forwarding</b> command from the <b>Monitor</b> menu however, disables the <b>Add, Remove, and OK</b> buttons.	Enables the <b>Trap Forwarding</b> command from the <b>Monitor</b> menu. Enables all functions in the <b>Configure Trap Forwarding</b> dialog box.
User Management	Allows you to create and the define users, groups, as well as assign privileges and views to groups.	Disables the <b>Users</b> command on the main <b>SAN</b> menu and the <b>Users</b> button on the main tool bar. Disables the <b>User List</b> button in the <b>Event Notification Setup</b> dialog box.	Enables the <b>Users</b> command on the <b>SAN</b> menu and the <b>Users</b> button on the main tool bar; however, disables the <b>Add, Edit, and Remove Users, Add and Remove Groups, and OK</b> buttons on the <b>Users</b> dialog box. Enables the <b>Edit Groups</b> button to display the <b>Group</b> dialog box (with <b>OK</b> button disabled).	Enables the <b>Users</b> command on the <b>SAN</b> menu and the <b>Users</b> button on the main tool bar. Enables all functions on the <b>Users</b> dialog box and the secondary <b>Group</b> dialog box.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
View Management	Allows you to create, edit, and delete views. Selecting from views should always be allowed unless restricted by the assignment of Views in the Group definition in the <b>Users</b> dialog box.	Disables the <b>Create View</b> , <b>Copy View</b> , <b>Edit View</b> , <b>Delete View</b> , and <b>Connectivity View</b> commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop. Allows you to select an assigned views but not create or change.	Enables the <b>Create View</b> and <b>Edit View</b> commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop; however, disables the <b>OK</b> button in the <b>Create View</b> and <b>Edit View</b> dialog boxes. Disables the <b>Copy View</b> , <b>Delete View</b> , and <b>Connectivity View &gt; Create</b> and <b>Refresh</b> commands. Allows you to select an assigned views but not create or change.	Activates all view commands in the <b>View &gt; Manage View</b> menu and the first tab header on the main desktop. Enables all functions in the dialog boxes.
Virtual Fabric	Allows you to configure virtual switches and fabrics.	Disables the <b>Virtual Switches</b> command from the <b>Configure</b> menu. However, this does not restrict the <b>Virtual Switches</b> command in the Element Managers.	Enables the <b>Virtual Switches</b> command in the <b>Configure</b> menu; however, disables the <b>Edit</b> and <b>OK</b> buttons in the <b>Virtual Switches</b> dialog box.	Enables the <b>Virtual Switches</b> command in the <b>Configure</b> menu. Enables all functions in the <b>Virtual Switches</b> dialog box.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Zoning Activation	Allows you to activate a zone set selected in the <b>Zoning</b> dialog box	Disables the <b>Activate</b> , <b>Deactivate</b> , and <b>Zoning Policies</b> buttons in the <b>Zoning</b> dialog box.	Same as no privilege.	Enables the <b>Activate</b> , <b>Deactivate</b> , and <b>Zoning Policies</b> buttons in the <b>Zoning</b> dialog box.
Zoning Fabric Libraries	Allows you to edit data in the Fabric Zone Libraries.	Removes the fabric library from the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Disables all the fabric libraries in the list of targets in the <b>Copy Into</b> right-click commands.	Includes the fabric library in the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Disables the <b>Save To</b> on the <b>Zoning</b> dialog box - <b>Active Zone Set</b> tab. Disables the right-arrow (for adding), left arrow (for removing), <b>New Zone</b> , <b>New Member</b> , <b>New Set</b> , <b>Import</b> , <b>OK</b> , and <b>Apply</b> buttons on the <b>Zoning</b> dialog box - <b>Zone Library</b> tab. Enables <b>Cancel</b> and <b>Help</b> buttons in the <b>Zoning</b> dialog box. Enables <b>Find</b> and Export buttons in the <b>Zoning</b> dialog box - <b>Zone Library</b> tab. Enables <b>Compare</b> and <b>Report</b> buttons in the <b>Zoning</b> dialog box - <b>Active Zone Set</b> tab. Enables all commands for the <b>Potential Member</b> right-click menu. Enables <b>Port Label</b> , <b>Search</b> , and <b>Properties</b> commands for the <b>Zones</b> right-click menu. Enables <b>Properties</b> command for the <b>Zone Sets</b> right-click menu. Enables <b>Properties</b> command for the <b>Zones in Zone Sets</b> right-click menu.	Includes the fabric library in the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Enables all functions on the dialog boxes.

**TABLE 56** Privileges and Application Behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Zoning Global Library (no mSAN and Router Fabric)	Allows you to add data in the Global Zone Library. Does not effect on Router Fabric or mSAN libraries.	Removes Global Library from the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Disables the <b>Global</b> command in the list of targets in the <b>Copy Into</b> right-click commands.	Includes the fabric library in the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Disables the <b>Save To</b> on the <b>Zoning</b> dialog box - <b>Active Zone Set</b> tab. Disables the right-arrow (for adding), left arrow (for removing), <b>New Zone</b> , <b>New Member</b> , <b>New Set</b> , <b>Import</b> , <b>OK</b> , and <b>Apply</b> buttons on the <b>Zoning</b> dialog box - <b>Zone Library</b> tab. Enables <b>Cancel</b> and <b>Help</b> buttons in the <b>Zoning</b> dialog box. Enables <b>Find</b> and <b>Export</b> buttons in the <b>Zoning</b> dialog box - <b>Zone Library</b> tab. Enables <b>Compare</b> and <b>Report</b> buttons in the <b>Zoning</b> dialog box - <b>Active Zone Set</b> tab. Enables all commands for the <b>Potential Member</b> right-click menu. Enables <b>Port Label</b> , <b>Search</b> , and <b>Properties</b> commands for the <b>Zones</b> right-click menu. Enables <b>Properties</b> command for the <b>Zone</b> Sets right-click menu. Enables <b>Properties</b> command for the <b>Zones in Zone Sets</b> right-click menu.	Includes the Global Library in the <b>Zoning Library</b> drop down list in the <b>Zoning</b> dialog box. Enables all functions on the dialog boxes.

## About User Groups and Access Levels

A user with administrative privileges can assign users to user groups. Five pre-configured user groups (System Administrator, Security Administrator, Maintenance, Operator, and Produce Administrator) are available with the application; however, System Administrators can also create user groups manually. Refer to [“Creating a User Group”](#) on page 94 for instructions.

**TABLE 57** Features and User Groups Access Levels

Feature	User Groups with Read/Write Access	User Groups with Read-Only Access
Active Session Management	System Administrator, Security Administrator	Operator, Maintenance, Product Administrator
Add/Delete Properties	System Administrator	Operator, Maintenance, Product Administrator
Advanced Call Home	System Administrator	
Backup	System Administrator, Maintenance, Product Administrator	Operator
Device Administration	System Administrator, Product Administrator	
Device Maintenance	System Administrator, Maintenance	
Device Operation	System Administrator, Operator	
Discover On/Off	System Administrator	Maintenance, Operator, Product Administrator
Discovery Setup	System Administrator	Maintenance, Operator, Product Administrator
E-mail Event Notification Setup	System Administrator, Maintenance	Operator, Product Administrator
Enterprise Fabric Mode	System Administrator, Security Administrator	Maintenance, Operator, Product Administrator
Event Management	System Administrator	Maintenance, Operator, Product Administrator
Export	System Administrator	Maintenance, Operator, Product Administrator
FabricBinding	System Administrator, Security Administrator	Maintenance, Operator, Product Administrator
Frame Sniffer	System Administrator	Maintenance, Operator, Product Administrator
Group Manager – Create Event Log	System Administrator	Maintenance, Operator, Product Administrator
Group Manager – Firmware Install	System Administrator	Maintenance, Operator, Product Administrator
Group Manager – Run Data Collection	System Administrator	Maintenance, Operator, Product Administrator
Import	System Administrator	Maintenance, Operator, Product Administrator
License Update	System Administrator	Maintenance, Operator, Product Administrator
Log Management	System Administrator	Maintenance, Operator, Product Administrator
LUN Management	System Administrator	Maintenance, Operator, Product Administrator
Map Editing	System Administrator	Maintenance, Operator, Product Administrator
Map HBA to Server	System Administrator	Maintenance, Operator, Product Administrator
Map Loop to Hub	System Administrator	Maintenance, Operator, Product Administrator
Map Port to Storage	System Administrator	Maintenance, Operator, Product Administrator

**TABLE 57** Features and User Groups Access Levels

Feature	User Groups with Read/Write Access	User Groups with Read-Only Access
Monitor Ethernet Event	System Administrator	Maintenance, Operator, Product Administrator
Performance	System Administrator	Maintenance, Operator, Product Administrator
Persist Fabric	System Administrator	Maintenance, Operator, Product Administrator
Planning	System Administrator	Maintenance, Operator, Product Administrator
PortFencing	System Administrator	Maintenance, Operator, Product Administrator
Properties Edit	System Administrator	Maintenance, Operator, Product Administrator
Remote Access	System Administrator, Security Administrator	Maintenance, Operator, Product Administrator
Report	System Administrator	Maintenance, Operator, Product Administrator
Security Admin	System Administrator, Security Administrator	Maintenance, Operator, Product Administrator
Setup Tools	System Administrator	Maintenance, Operator, Product Administrator
Show Route	System Administrator	Maintenance, Operator, Product Administrator
Shutdown	System Administrator	Maintenance, Operator, Product Administrator
SNMP Agent Configuration	System Administrator	Maintenance, Operator, Product Administrator
Software Configuration Properties	System Administrator	Maintenance, Operator, Product Administrator
Trap Forwarding	System Administrator	Maintenance, Operator, Product Administrator
User Management	System Administrator, Security Administrator	Maintenance, Operator, Product Administrator
View Management	System Administrator	Maintenance, Operator, Product Administrator
VirtualFabric	System Administrator	Maintenance, Operator, Product Administrator
Zoning Activation	System Administrator	Maintenance, Operator, Product Administrator
Zoning Fabric Libraries	System Administrator	Maintenance, Operator, Product Administrator
Zoning Global Library	System Administrator	Maintenance, Operator, Product Administrator

# Advanced Call Home Event Tables

---

## In this Appendix

This section provides information about the specific events that display when using Advanced Call Home. This information is shown in the following Event Tables.

- [Call Home Event Table .....](#) 288
- [# CONSRV Events .....](#) 289
- [# Thermal Event Reason Codes .....](#) 290
- [# QLogic Events .....](#) 290
- [# Brocade Events.....](#) 291

**TABLE 58** Call Home Event Table

Event Reason Code	FRU Code/Event Type	Description	Severity
10	None/SW	Login Server unable to synchronize databases.	2
11	None/SW	Login Server database found to be invalid.	2
20	None/SW	Name Server unable to synchronize databases.	2
21	None/SW	Name Server database found to be invalid.	2
40	None/SW	Operator panel has failed.	2
50	None/SW	Management Server unable to synchronize databases.	2
51	None/SW	Management Server database found to be invalid.	2
60	None/SW	Fabric Controller unable to synchronize databases.	2
61	None/SW	Fabric Controller database found to be invalid.	2
90	None/SW	Database replication time out.	2
153	PWR/HW	ifcpBackupActivated.	4
154	PWR/HW	ifcpRemoteConnectionDown.	4
155	PWR/HW	CallHomeRPortError	3
200	None/SW	Power supply AC voltage failure.	3
201	PWR/HW	Power supply DC voltage failure.	3
202	PWR/HW	Power supply thermal failure.	3
208	PWR/HW	Power supply false shutdown.	3
300	FAN/HW	A cooling fan propeller has failed.	3
301	FAN/HW	A cooling fan propeller has failed (two failed propellers).	3
302	FAN/HW	A cooling fan propeller has failed.	3
303	FAN/HW	A cooling fan propeller has failed.	3
304	FAN/HW	A cooling fan propeller has failed.	3
305	FAN/HW	A cooling fan propeller has failed.	3
306	FAN/HW	A cooling fan propeller in FAN2 FRU type has failed.	3
307	FAN/HW	A cooling fan propeller in FAN2 FRU type has failed.	3
322	FAN/HW	Front top fan FRU failed.	3
323	FAN/HW	Front bottom fan FRU failed.	3
324	FAN/HW	Rear top fan FRU failed.	3
400	CTP/HW	Power-up diagnostic failure.	3
411	CTP/SW	Firmware fault occurred.	3
413	CTP/HW	Backup CTP power-on self test failure.	3

**TABLE 58** Call Home Event Table

Event Reason Code	FRU Code/Event Type	Description	Severity
414	CTP/HW	Backup CTP failure.	3
419	CTP/INFO	Board NVRAM failure.	3
420	CTP/HW	CTP non-volatile memory failure.	3
425	CTP/HW	CTP DRAM mismatch.	3
427	CTP/HW	Utility Bus Errors detected by backup CTP.	3
433	CTP/SW	Non-recoverable Ethernet fault.	3
440	CTP/HW	Embedded Port fatal error.	3
473	CTP/SW	CTP shutdown due to failure.	3
488	CTP/HW	Critical CTP failure on single CTP system.	3

**TABLE 59** # CONSRV Events

Event Reason Code	FRU Code/Event Type	Description	Severity
504	DVP/LIM/HW	EOS: Port module failure.	3
506	DVP/PORT	Fibre Channel port failure	3
509	DVP/PORT	Fibre Channel path failure.	0
511	LIM/DVP	LIM SPP failure.	3
514	DVP/ LIM/PORT	SFP/XFP optics failure.	3
517	LIM	LIM SPP Offline.	3
530	LIM/DVP	LIM Power-up diagnostic failure.	3
604	SBAR/SWM/HW	EOS: SBAR module failure.	3
607	SBAR/SWM/HW	EOS: Switch contains no operational SBAR cards.	4
622	SBAR/INFO	SWM powered off	0
623	SBAR/INFO	SWM powered on	0
624	SBAR/INFO	SWM disengaged	0

**TABLE 60** # Thermal Event Reason Codes

Event Reason Code	FRU Code/Event Type	Description	Severity
800	DVP/LIM/HW	High temperature warning.	3
801	DVP/LIM/HW	Critically hot temperature warning.	3
802	DVP/LIM/HW	EOS: Port card shutdown due to thermal violations.	3
805	SWM/SBAR/HW	High temperature warning.	3
806	SWM/SBAR/HW	Critically hot temperature warning.	3
807	SWM/SBAR/HW	EOS: SBAR module shutdown due to thermal violations.	3
810	CTP/HW	High temperature warning.	3
811	CTP/HW	Critically hot temperature warning.	3
812	CTP/HW	CTP shutdown due to thermal violations.	3
850	CTP/HW	System shutdown due to CTP thermal threshold violations.	4

**TABLE 61** # QLogic Events

Event Reason Code	FRU Code/Event Type	Description	Severity
895	1003.0017	A zone member defined by domain ID and port was received within a management server AZSD command with a port number out of range.	4
903	1003.0022	Modifications were being made to the security database while a security set was being activated or deactivated from a remote switch.	4
907	1003.0031	A device supporting management server has sent an Activate Zoneset Direct \$(AZSD) command that did not follow the expected standard layout.	4
992	3003.0003	Diagnostic testing has determined that there is a failure on specified I/O blade. The blade did not pass the Power-On-Self-Test (POST).	4
993	3004.0001	A non-fatal hardware error was discovered during the Power-On-Self-Test (POST) phase of startup.	4
994	3004.0002	Diagnostic testing has determined that there is a partial failure on specified I/O blade. Most likely at least one of the ports did not pass the Power-On-Self-Test (POST).	4
999	6001.0001	The Hotreset command has failed due to insufficient memory on the switch. The switch has been returned to its state before the Hotreset command was entered.	4

**TABLE 62** # Brocade Events

Event Reason Code	FRU Code/Event Type	Description	Severity
1009	MS-1009	Error in registered link incident record (RLIR)	4
1050	EM-1050	FRU removed	2
1426	FW-1426	Faulty or Missing Power supply	3
1427	FW-1427	Faulty Power supply	3
1428	FW-1428	Missing Power supply	3
1429	FW-1429	Problem in power supply arrangement	3
1430	FW-1430	Faulty Temperature sensors	3
1431	FW-1431	Faulty fans	3
1432	FW-1432	Faulty WWN Cards	3
1433	FW-1433	Faulty CPs	3
1434	FW-1434	Faulty Blades	3
1402	FW-1402	Flash usage is out of range	3
1436	FW-1436	Marginal port	3
1437	FW-1437	Faulty Port	3
1438	FW-1438	Faulty or Missing SFPs	3

## **G** In this Appendix

# B Model Considerations

---

## In this Appendix

This section provides information specific to B model devices.

## B Model Supported Traps

The following list details the B model supported traps that display in the master log when triggered.

**TABLE 63** B Model Supported Traps

Trap	Event Type
ConnUnitEventTrap	SNMP Trap Event
ConnUnitStatusChange	Call Home Event
FruStatusChanged	Call Home Event
RLIRLinkFailureIncident	Call Home Event

H

# Glossary

---

This glossary includes terms and definitions from:

- *American National Standard Dictionary for Information Systems* (ANSI X3.172-1990), copyright 1990 by the American National Standards Institute (ANSI). Copies can be purchased from the American National Standards Institute, 25 West 42nd Street, New York, NY 10036. Definitions from this text are identified by (A).
- *ANSI/EIA Standard - 440A: Fiber Optic Terminology*, copyright 1989 by the Electronic Industries Association (EIA). Copies can be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue N.W., Washington, D.C. 20006. Definitions from this text are identified by (E).
- *IBM Dictionary of Computing* (ZC20-1699). Definitions from this text are identified by (D).
- *Information Technology Vocabulary*, developed by Subcommittee 1 (SC1), Joint Technical Committee 1 (JTC1), of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). Definitions of published parts of this vocabulary are identified by (I). Definitions taken from draft international standards, committee drafts, and working papers developed by ISO/IEC SC1/JTC1 are identified by (T), indicating that final agreement has not been reached among the participating national bodies of SC1.

## A

### accelerator

A short-cut keystroke method to perform a menu operation. Menu options may have accelerator keys listed to the right of the menu option. Use the listed accelerator to perform the menu option's function when no menu is selected for the window (*D*).

### access

The ability and means necessary to store data in, to retrieve data from, to transfer data into, to communicate with, or to make use of any resource of a storage product, a system, or area such as random access memory (RAM) or a register.

### access control

A list of all products that can access other products across the network and the permissions associated with that access. See also [persistent binding](#); [zoning](#).

### access time

The amount of time, including seek time, latency, and controller time, necessary for a storage product to retrieve information.

### active configuration

In FICON management style, the director or switch configuration that is determined by the status of the connectivity attributes.

### active field-replaceable unit

Active FRU. A FRU that is currently operating as the active, and not the backup FRU. See also [backup field-replaceable unit](#).

### active FRU

See [active field-replaceable unit](#).

### active port address matrix

In FICON management style, an active port address matrix is the port address matrix that is currently active or operational on an attached director or switch.

### active zone set

A single zone set that is active in a multiswitch fabric and is created when a specific zone set is enabled. This zone set is compiled by checking for undefined zones or aliases. See also [zone](#); [zone set](#).

### adapter

A printed circuit assembly which transmits user data (I/Os) between the host system's internal bus and the external Fibre Channel link and vice versa. Also called an I/O adapter, host adapter, or FC adapter.

### address

(1) To refer to a product or an item of data by its address (*A, I*). (2) The location in a computer where data is stored. (3) In data communication, the unique code assigned to each product or computer connected to a network. (4) The identifier of a location, source, or destination (*D*).

### address name

Synonym for [port name](#).

### address resolution protocol

ARP. The protocol by which a host computer maintains a cache of address translations, allowing the physical address of the computer to be derived from the Internet address (*D*).

### agent

Software that processes queries on behalf of an application and returns replies.

### alarm

(1) A notification of an abnormal condition within a system that provides an indication of the location or nature of the abnormality to either a local or remote alarm indicator. (2) A simple network management protocol (SNMP) message notifying an operator of a network or product problem.

### alias

A nickname representing a world-wide name (WWN).

### allowed connection

In FICON management style, in a director or switch, the attribute that when set, establishes dynamic connectivity capability. *Contrast with* [blocked connection](#). See [connectivity attribute](#). See also [dynamic connectivity](#); [unblocked connection](#).

### allowed port connection

In FICON management style, this attribute establishes dynamic connectivity capability.

### AL\_PA

See [arbitrated loop physical address](#).

**American National Standard Code for Information Interchange**

ASCII. A standard character set consisting of 7-bit coded characters (8-bit including parity check) used for information exchange between systems and equipment (D).

**American National Standards Institute**

ANSI. A national organization consisting of producers, consumers, and general interest groups that establishes procedures by which accredited organizations create and maintain industry standards in the United States (A).

**ANSI**

See [American National Standards Institute](#).

**API**

See [application program interface](#).

**application**

(1) The use to which a data processing system is put, for example, a payroll application, an airline reservation application, or a network application. (2) A collection of software components used to perform specific types of work on a computer (D).

**application client**

The source object of the small computer system interface (SCSI) commands and destination for the command responses.

**application program**

(1) A program that is specific to the solution of an application problem. Synonymous with application software. (2) A program written for or by a user that applies to the user's work, such as a program that does inventory control or payroll. (3) A program used to connect and communicate with stations in a network, enabling users to perform application-oriented activities (I).

**application program interface**

API. A set of programming functions and routines that provides access between protocol layers, such as between an application and network services.

**application-specific integrated circuit**

ASIC. An asynchronous transfer mode (ATM) local area network/ wide area network (LAN/WAN) circuit using cell relay transport technology. ASICs are designed for a specific application or purpose, such as implementing the lower-layer Fibre Channel protocol (FC-0). They are particularly suited to sending video and audio information, as well as text. ASICs differ from general-purpose products such as memory chips or microprocessors.

**arbitrated loop**

One of the three connection topologies offered by Fibre Channel protocol. Up to 126 node ports and one fabric port can communicate without the need for a separate switched fabric.

**arbitrated loop physical address**

AL\_PA. A 1-byte value used in the arbitrated loop topology that identifies loop ports (L\_Ports). This value then becomes the last byte of the address identified for each public L\_Port on the loop.

**arbitration**

Process of selecting one product from a collection of products that request service simultaneously.

**archive**

(1) To copy files to a long-term storage medium for backup. (2) Removing data, usually old or inactive files, from a system and permanently storing the data on removable media to reclaim system hard disk space.

**area**

The second byte of the node port (N\_Port) identifier.

**ARP**

See [address resolution protocol](#).

**array**

Two or more disk drives connected to a host, and connected and configured such that the host perceives the disk drives to be one disk.

**ASCII**

See [American National Standard Code for Information Interchange](#).

**ASIC**

See [application-specific integrated circuit](#).

**attribute**

In FICON management style, the connection status of the address on a configuration matrix: allowed, blocked, or prohibited.

**Audit Log**

Log summarizing actions (audit trail) made by the user.

Director or switch *Audit Log*. Log displayed through the Element Manager application that provides a history of all configuration changes made to an individual director or switch from the respective Element Manager application, a simple network management protocol (SNMP) management workstation, a Fibre Connection (FICON) or open systems host, or the maintenance port. This information is useful for administrators and users.

**availability**

The accessibility of a computer system or network resource.

**B**

**b**

See [bit](#).

**B**

See [byte](#).

**backup**

To copy files to a second medium (disk or tape) as a precaution in case the first medium fails.

**backup diskette**

A diskette that contains duplicate information from an original diskette. The backup diskette is used in case information on the original diskette is unintentionally changed or destroyed (*D*).

**backup field-replaceable unit**

Backup FRU. When an active FRU fails, an identical backup FRU takes over operation automatically (failover) to maintain director or switch and Fibre Channel link operation. See also [active field-replaceable unit](#).

**backup FRU**

See [backup field-replaceable unit](#).

**bandwidth**

(1) The amount of data that can be sent over a given circuit. (2) A measure of how fast a network can move information, usually measured in Hertz (Hz).

**baud**

The unit of signaling speed, expressed as the maximum number of times per second the signal can change the state of the transmission line or other medium. The units of baud are seconds to the negative 1 power. Note: With Fibre Channel scheme, a signal event represents a single transmission bit.

**BB\_Credit**

See [buffer-to-buffer credit](#).

**beaconing**

Use of light-emitting diodes (LEDs) on ports, port cards, field-replaceable units (FRUs), and directors to aid in the fault-isolation process. When enabled, active beaconing causes LEDs to flash, to enable the user to locate field-replaceable units (FRUs), switches, or directors in cabinets or computer rooms.

**ber**

See [bit error rate](#).

**bidirectional**

In Fibre Channel protocol, the capability to simultaneously communicate at maximum speeds in both directions over a link.

**bit**

Abbreviated as b. (1) Binary digit, the smallest unit of data in computing, with a value of zero or one (*D*). (2) A bit is the basic data unit of all digital computers. It is usually part of a data byte or data word; however, a single bit can be used to control or read logic ON/OFF functions. (3) A bit is a single digit in a binary number. Bits are the basic unit of information capacity on a computer storage product. Eight bits equals one byte.

**bit error rate**

Abbreviated as ber. Ratio of received bits that contain errors to total of all bits transmitted.

**blocked connection**

In FICON management style, in a director or switch, the attribute that, when set, removes the communication capability of a specific port. A blocked address is disabled so that no other address can be connected to it. A blocked attribute supersedes a dedicated or prohibited attribute on the same address. *Contrast with* [allowed connection](#); [unblocked connection](#). See [connectivity attribute](#). See also [dynamic connection](#); [dynamic connectivity](#).

**blocked port**

In a director or switch, the attribute that when set, removes the communication capability of a specific port. A blocked port continuously transmits the offline sequence.

**boot**

(1) To start or restart a computer. (2) Loading the operating system.

**B\_Port**

See [bridge port](#).

**bps**

Bits per second.

**Bps**

Bytes per second.

**bridge**

(1) An attaching product that connects two local area network (LAN) segments to allow the transfer of information from one LAN segment to the other. A bridge can connect the LAN segments directly by network adapters and software in a single product, or can connect network adapters in two products through software and use of a telecommunication link between the two adapters (*D*). (2) A functional unit that connects two LANs that use the same logical link control protocol, but may use different media access control protocols (*T*). *Contrast with* [router](#). (3) A product that connects and passes packets between two network segments that use the same communications protocol.

**bridge group**

A bridge and the collection of products connected to it.

**bridge port**

B\_Port. (1) In Fibre Channel protocol, a fabric inter-element port used to connect bridge products with E\_Ports on a switch. B\_Ports provide a subset of E\_Port functionality. (2) Physical interface between the fabric (switch) and a bridge product. The interface is identical to an expansion port (E\_Port), but it does not participate in full expansion port protocols. As such, it does not assign domain IDs or participate in routing protocol. See also [expansion port](#); [fabric loop port](#); [fabric port](#); [generic port](#); [hub port](#); [node loop port](#); [node port](#); [segmented expansion port](#).

**broadcast**

A method of sending an SNMP request for information to all the products on a subnet that uses a single special request. Because of its efficiency, the SAN Management application sets its default method of discovery to broadcast. However, a network administrator may disable this method on the network router.

**buffer**

Storage area for data in transit. Buffers compensate for differences in processing speeds between products.

**buffer-to-buffer credit**

BB\_Credit. (1) The maximum number of receive buffers allocated to a transmitting node port (N\_Port) or fabric port (F\_Port). Credit represents the maximum number of outstanding frames that can be transmitted by that N\_Port or F\_Port without causing a buffer overrun condition at the receiver. (2) The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving product. BB\_Credit can be adjustable to provide different levels of compensation.

**bus**

The path that carries data between the computer (microprocessor) and peripheral products. An IDE interface cable and a small computer system interface (SCSI) cable are both examples.

**bypassed port**

If a port is bypassed, all serial channel signals route past the port. A product attached to the port cannot communicate with other products in the loop.

**byte**

Abbreviated as B. A byte generally equals eight bits, although a byte can equal from four to ten bits.

## C

### cache

Random access memory (RAM) that is used by the redundant array of independent disks (RAID) controller to increase I/O throughput. If write-back caching is enabled, this RAM can contain data that is not yet written to the disks in the array. In normal circumstances, this data is flushed from the RAM to the disk drives in the array with a maximum latency of 64 ms. If power fails to the subsystem (preventing the data from being written to the disk drives in the array), the battery holds the data for approximately 72 hours. If power is restored within that period, the data is flushed into the array and operation continues normally. If power has not been restored within 72 hours the data is lost.

### cache memory

A memory subsystem that stores recently used instructions and data for fast access. The larger the cache, the more information that can be stored, and the fewer time-consuming memory accesses a central processing unit (CPU) must make to complete a task. Cache is very fast memory, typically static random access memory (SRAM).

### call-home

Product feature which enables the server platform to automatically contact a support center and report system problems. The support center server accepts calls from the server platform logs reported events, and can notify one or more support center representatives.

### capacity

The amount of information, measured in bytes, that can be stored on a hard drive.

### cascade

Linking two or more Fibre Channel switches to form a larger switch or fabric. The switched link through fiber cables attached between one or more expansion ports (E\_Ports). See *also* [expansion port](#).

### cell

In FICON management style, in a port address matrix, a cell is the intersection point between a horizontal port address and a vertical port address. A selected cell is indicated by the cell cursor.

### central memory module card

CMM. In the Director, a circuit card that provides the storage area for Fibre Channel ports to deposit and retrieve Fibre Channel frames. Each port is allocated a portion of this memory divided into a fixed number of frame buffers.

### central processing unit

CPU. The heart of the computer, this is the component that actually executes instructions.

### chained

Two directors or switches that are physically attached.

### channel wrap test

A diagnostic procedure that checks S/390 host-to-director or host-to-switch connectivity by returning the output of the host as input. The test is host-initiated and transmits Fibre Channel frames to a director or switch port. A director or switch port enabled for channel wrapping echoes the frame back to the host.

### Class 2 Fibre Channel service

Provides a connectionless (not dedicated) service with notification of delivery or nondelivery between two node ports (N\_Ports).

### Class 3 Fibre Channel service

Provides a connectionless (not dedicated) service without notification of delivery or nondelivery between two node ports (N\_Ports). *Synonymous with* [datagram](#).

### Class F Fibre Channel service

Used by switches to communicate across interswitch links (ISLs) to configure, control, and coordinate a multswitch fabric.

### Class of Fibre Channel service

Defines the level of connection dedication, acknowledgment, and other characteristics of a connection.

### client

A node that requests network services from a server. Typically the node is a personal computer (PC).

### client/server computing

Architectural model that functionally divides that execution of a unit of work between activities initiated by an end user or program (client) and those maintaining data (servers). Originally thought to make mainframes obsolete.

**cluster**

A group of processors interconnected by a high-speed network (typically dedicated) for increased reliability and scalability. Clusters are groupings of multiple servers in which information is shared among systems. When a server in a cluster fails, one of the other servers in the cluster assumes the responsibility of the failed server, thereby ensuring server, application, and data availability.

**CMM**

See [central memory module card](#).

**command**

(1) A character string from an external source to a system that represents a request for system action. (2) A request from a terminal to perform an operation or execute a program. (3) A value sent through an I/O interface from a channel to a control unit that specifies the operation to be performed (*D*). A selection on a dialog box or elsewhere in the user interface that causes the SAN Management application to perform a task.

**community name (SNMP)**

A name that represents an simple network management protocol (SNMP) community that the agent software recognizes as a valid source for SNMP requests. A product recognizes a management station as a valid recipient for trap information when the station's community names are configured.

**community profile**

Information that specifies which management objects are available to what management domain or simple network management protocol (SNMP) community name.

**community (SNMP)**

A relationship between an simple network management protocol (SNMP) agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

**community strings**

The community name that is contained in each SNMP message. It is not secure and there is no way of keeping the contents private or for determining if a message has been changed or replayed. The community string value is not encrypted.

**component**

(1) Hardware or software that is part of a functional unit. (2) A functional part of an operating system; for example, the scheduler or supervisor (*D*).

**computer**

A programmable machine that responds to a specific set of instructions in a well-defined manner and executes a prerecorded list of instructions (a program). Computers are both electronic and digital and are made up of both hardware (the actual machine-wires, transistors, and circuits) and software (instructions and data).

**concurrent firmware upgrade**

Firmware is upgraded without disrupting switch operation.

**configuration data**

The collection of data that results from configuring product and system operating parameters. For example, configuring operating parameters, SNMP agent, and port configurations through the Element Manager application, results in a collection of configuration data. Configuration data includes: identification data, port configuration data, operating parameters, and SNMP configuration. A configuration backup file is required to restore configuration data if the control processor (CTP) card in a nonredundant ED-5000 Director is removed and replaced.

**connectivity**

The ability of products to link together.

**connectivity attribute**

In FICON management style, the characteristic that determines port address status for the director or switch. See [allowed connection](#); [blocked connection](#); [connectivity control](#); [dynamic connection](#); [dynamic connectivity](#); [unblocked connection](#).

**connectivity capability**

(1) The capability that allows attachment of a product to a system without requiring physical reconfiguration of either the product or the interconnections. (*D*)

**connectivity control**

In FICON management style, in a director or switch, the method used to change port address connectivity attributes and determine the communication capability of the link attached to the port (*D*). See *also* [active port address matrix](#); [connectivity attribute](#).

**connector**

*Synonym for* optical fiber connector.

**console**

See [personal computer](#); [segmented loop port](#).

**context menu**

See [shortcut menu](#).

**control processor card**

CTP card. Circuit card that contains the director or switch microprocessor. The CTP card also initializes hardware components of the system after power-on. The card may contain an RJ-45 twisted pair connector.

**control unit port**

CUP. An internal director or switch port on the control processor (CTP) card (labelled FE) that communicates with channels to report error conditions and link initialization (D).

**CRC**

See [cyclic redundancy check](#).

**credit**

See [buffer-to-buffer credit](#).

**CTP card**

See [control processor card](#).

**CUP**

See [control unit port](#).

**customer support**

Synonym for [technical support](#).

**cyclic redundancy check**

CRC. System of error checking performed at both the sending and receiving station using the value of a particular character generated by a cyclic algorithm. When the values generated at each station are identical, data integrity is confirmed.

**D**

**DASD**

See [direct access storage device](#).

**database**

A collection of data with a given structure for accepting, storing, and providing on-demand data for multiple users (T).

**data center**

A collection of servers and data storage products, usually in one location, administered by an information technology/information services (IT/IS) manager.

**data integrity**

Refers to the validity of data. Data integrity can be compromised in a number of ways including human errors when data is entered, errors that occur when data is transmitted from one computer to another, software bugs or viruses, hardware malfunctions (disk crashes), and natural disasters (fires and floods). There are many ways to minimize these threats to data integrity such as backing up data regularly, controlling access to data via security mechanisms, designing user interfaces that prevent the input of invalid data, and using error detection and correction software when transmitting data.

**data recovery**

Salvaging data stored on damaged media, such as magnetic disks and tapes. There are a number of software products that can help recover data damaged by a disk crash or virus. Of course, not all data is recoverable, but data recovery specialists can often restore a surprisingly high percentage of the data on damaged media.

**datagram**

Synonym for [Class 3 Fibre Channel service](#).

**default**

Pertaining to an attribute, value, or option that is assumed by a system when none is explicitly specified (D, I).

**default zone**

A zone that contains all attached products that are not members of a separate active zone.

**destination**

A point or location, such as a processor, director or switch, or server, to which data is transmitted (D).

**destination address**

D\_ID. An address identifier that indicates the targeted destination of a data frame.

**device**

(1) Product, connected to a managed director or switch. See also [node](#). (2) Mechanical, electrical, or electronic hardware with a specific purpose. (D)

**device number**

In a channel subsystem, four hexadecimal digits that uniquely identify an I/O product (D).

**device type**

Identifier used to place products in the Physical Map (i.e. switch, hub, storage, etc.).

**diagnostics**

(1) The process of investigating the cause or nature of a problem in a product or system. (2) Procedures or tests used by computer users and service personnel to diagnose hardware or software problems (*D*).

**dialog box**

A pop-up window in the user interface with informational messages or fields to be modified or completed with desired options.

**D\_ID**

See [destination address](#).

**digital transmission**

Information is converted to binary computer code (a series of 0s and 1s). The information is sent in this format and then converted into its original format when it reaches its destination.

**direct access storage device**

DASD. (1) Generic classification for a storage peripheral that can respond directly to random requests for information. Usually refers to a disk drive. (2) A storage product that provides direct access to data, and in which access time is independent of data location.

**director**

An intelligent, highly-available, Fibre Channel switch providing any-to-any port connectivity between nodes (end devices) on a switched fabric. The director sends data transmissions (data frames) between nodes in accordance with the address information present in the frame headers of those transmissions.

**disaster recovery**

A program that is designed to help companies get back to normal activities after a catastrophic interruption. Through failover to a parallel system, or by restoration of the failed system, disaster recovery restores the system to its normal operating mode.

**discovery**

The process by which the SAN Management application detects products in a SAN. See also [out-of-band discovery](#).

**diskette**

A thin magnetic disk enclosed in a plastic jacket, which is removable from a computer and is used to store and transport data (*D*).

**diskette drive**

The hardware mechanism by which a computer reads data from and writes data to removable diskettes (*D*).

**disk operating system**

DOS. The computer program that controls the organization of data, files, and processes on the computer.

**DNS name**

Domain name system or domain name service. Host or node name for a managed product that is translated to an Internet protocol (IP) address through a domain name server.

**domain**

A Fibre Channel term describing the most significant byte in the node port (N\_Port) identifier for the Fibre Channel product. It is not used in the Fibre Channel small computer system interface (FC-SCSI) hardware path ID. It is required to be the same for all SCSI targets logically connected to a Fibre Channel adapter.

**domain ID**

Domain identifier. A number that uniquely identifies a switch in a multswitch fabric. A distinct domain ID is automatically allocated to each switch in the fabric by the principal switch. The preferred domain ID is the domain ID value that a switch requests from the principal switch. If the value has not been allocated to another switch in the fabric, it is granted by the principal switch and becomes the requesting switch's active domain ID. The active domain ID is the domain ID that has been assigned by the principal switch and that a switch is currently using.

**domain name server**

In transmission control protocol/Internet protocol (TCP/IP), a server program that supplies name-to-address translation by mapping domain name to internet addresses (*D*).

**DOS**

See [disk operating system](#).

**drop-down menu**

A menu that appears when a heading in a navigation bar is clicked on with the mouse. The objects that appear in the drop-down menus are organized by their headings in the navigation bar.

**dump**

The file that is created when the director detects a software fault. It contains various data fields that, when extracted, assist in the debugging of software.

**dynamic connection**

A connection between two ports, established or removed by the directors and that, when active, appears as one continuous link. See [connectivity attribute](#). See also [allowed connection](#); [blocked connection](#); [dynamic connectivity](#); [unblocked connection](#).

**dynamic connectivity**

The capability that allows connections to be established and removed at any time.

**dynamic random access memory**

DRAM. Random access memory that resides in a cell comprised of a capacitor and transistor. DRAM data deteriorates (that is, is dynamic) unless the capacitor is periodically recharged by the controlling microprocessor. DRAM is slow, but relatively inexpensive (*D*). Contrast with [static random access memory](#).

## E

**EFCM**

Enterprise Fabric Connectivity Manager application. Management software that provides easy, centralized management of a SAN and quick access to all device configuration applications.

**electronic data interchange**

EDI. The electronic transfer of preformatted business documents, such as purchase orders and bills of lading, between trading partners.

**Electronic Industries Association**

EIA. The governing body that publishes recommended standards for physical products and associated interfaces. For example, RS-232 is the EIA standard that defines computer serial port connectivity (*D*).

**electronic mail**

E-mail. Any communications service that permits the electronic transmission and storage of messages and attached or enclosed files.

**Element Manager application**

Application that implements the management user interface for a director or switch. (1) In your SAN management application application, the software component that provides a graphical user interface for managing and monitoring switch products. When a product instance is opened from your SAN management application, the corresponding Element Manager application is invoked.

**e-mail**

See [electronic mail](#).

**enhanced availability feature**

EAF. A backup field-replaceable unit (backup FRU) that is ordered and installed to provide redundancy and reduce disruption in case of failure (*D*).

**enterprise**

The entire storage system. The series of computers employed largely in high-volume and multi-user environments such as servers or networking applications; may include single-user workstations required in demanding design, engineering and audio/visual applications.

**Enterprise Fabric Connectivity Manager application**

See [EFCM](#).

**Enterprise Systems Architecture**

ESA™. A computer architecture introduced by IBM in 1988 as ESA/370. The architecture added access registers to improve virtual memory management and increase storage from 2 gigabyte to 6 terabytes. The architecture was enhanced with the introduction of ESA/390 in 1990 (*D*).

**Enterprise Systems Connection**

ESCON™. An IBM architecture, technology, and set of products and services introduced in 1990 that provides a dynamically connected environment using fiber-optic cables as the data transmission medium (*D*).

**Enterprise Systems Connection Director**

ESCON™ Director. A device that provides connectivity capability and control for attaching any two links to each other through the ESON channel. Specifically, any of the hardware products provided for interconnecting IBM-compatible mainframe equipment through the proprietary ESCON channel connection. IBM's model numbers for ESCON directors include the 9031 and 9033.

**E\_Port**

See [expansion port](#).

**erase**

To remove electrically or magnetically stored data, leaving the space where the data was stored unoccupied (D).

**error-detect time-out value**

E\_D\_TOV. The time the switch waits for an expected response before declaring an error condition.

**error log**

See [master log](#).

**error message**

Indication that an error has been detected (D). See also [information message](#); [warning message](#).

**ESA™**

See [Enterprise Systems Architecture](#).

**ESCON™**

See [Enterprise Systems Connection](#).

**ESCON™ Director**

See [Enterprise Systems Connection Director](#).

**Ethernet**

A widely implemented local area network (LAN) protocol that uses a bus or star topology and serves as the basis for the Institute of Electrical and Electronics Engineers (IEEE) 802.3 standard, which specifies the physical and software layers.

**Ethernet hub**

A product used to connect a server and the switches it manages.

**event code**

A three-digit number that specifies the exact event that occurred. This code provides information on system failures, such as hardware failures, failure locations, or general information on normal system events.

**event log**

Displays errors related to SAN management, such as SNMP traps or Client-Server communications.

**event notification**

A process by which the SAN Management application informs remote users and workstations of certain classes of events that occur on the system. E-mail notification and the configuration of simple network management protocol (SNMP) trap recipients are two examples of remote notification programs that can be implemented through the application.

**exchange**

A term that refers to one of the Fibre Channel protocol "building blocks," composed of one or more nonconcurrent sequences.

**expansion port**

E\_Port. Physical interface on a Fibre Channel switch within a fabric, that attaches to an E\_Port on another Fibre Channel switch through an interswitch link (ISL) to form a multiswitch fabric. See also [fabric loop port](#); [fabric port](#); [hub port](#); [node loop port](#); [node port](#).

**explicit fabric login**

The process by which a node port (N\_Port) learns the characteristics of the fabric to which it is attached by sending a fabric login command (FLOGI) frame to the fabric port (F\_Port) address FFFFFE (hexadecimal).

**extended distance feature**

XDF. A means to extend the propagation distance of a fiber-optic signal.

**F****fabric**

Entity that is capable of routing (switching) Fibre Channel frames, using the destination ID information in the Fibre Channel frame header accompanying the frames.

**fabric element**

Any active director, switch, or node in a switched fabric.

**fabric group**

A collection of interconnected SAN devices discovered by the SAN Management application. Fabric groups display with a blue background on the Physical Map.

**fabric login**

The process by which node ports (N\_Ports) establish their operating parameters. During fabric login, the presence or absence of a fabric is determined, and paths to other N\_Ports are mapped. Specific operating characteristics for each port, such as buffer-to-buffer credit (BB\_Credit) and data frame size, are also established.

**fabric login command**

FLOGI. The command that establishes the initial operating parameters and topology for a fabric. The command is accepted by a fabric port (F\_Port) (D).

**fabric loop port**

FL\_Port. A fabric port (F\_Port) that contains arbitrated loop (AL) functions associated with the Fibre Channel arbitrated loop (FC-AL) topology. The access point of the fabric for physically connecting an arbitrated loop of node loop ports (NL\_Ports). See also [expansion port](#); [fabric port](#); [hub port](#); [node loop port](#); [node port](#).

**fabric mode**

See [interoperability mode](#).

**fabric port**

F\_Port. Physical interface within the fabric that connects to a node port (N\_Port) through a point-to-point full duplex connection. See also [expansion port](#); [fabric loop port](#); [hub port](#); [node loop port](#); [node port](#).

**fabric services**

The services that implement the various Fibre Channel protocol services that are described in the standards. These services include the fabric controller (login server), name server, and server platform.

**fabric switches**

A product that allows communication between multiple products using Fibre Channel protocols. A fabric switch enables the sharing bandwidth and end-nodes using basic multiplexing techniques.

**failover**

Automatic and nondisruptive transition of functions from an active field-replaceable unit (FRU) that has failed to a backup FRU.

**FC**

See [Fibre Channel](#).

**FC-0**

The Fibre Channel layer that describes the physical link between two ports, including the transmission media, transmitter and receiver circuitry, and interfaces (D). This consists of a pair of either optical fiber or electrical cables (link media) along with transceiver circuitry which work together to convert a stream of bits at one end of the link to a stream of bits at the other end.

**FC-1**

Middle layer of the Fibre Channel physical and signaling interface (FC-PH) standard, defining the 8B/10B encoding/decoding and transmission protocol.

**FC-2**

The Fibre Channel layer that specifies the signaling protocol, rules, and mechanisms required to transfer data blocks. The FC-2 layer is very complex and provides different classes of service, packetization, sequencing, error detection, segmentation, and reassembly of transmitted data (D).

**FC-3**

The Fibre Channel layer that provides a set of services common across multiple node ports (N\_Ports) of a Fibre Channel node. The services are not commonly used and are essentially reserved for Fibre Channel architecture expansion (D).

**FC-4**

The Fibre Channel layer that provides mapping of Fibre Channel capabilities to upper level protocols (ULP), including Internet protocol (IP) and small computer system interface (SCSI) (D).

**FCA**

See [Fibre Channel Association](#).

**FC-AL**

See [Fibre Channel arbitrated loop](#).

**FC adapter**

Fibre Channel adapter. See [host bus adapter](#).

**FCC**

Federal Communications Commission.

**FCC-IOC**

See [Fibre Channel I/O controller](#).

**FCFE**

See [Fibre Channel fabric element](#).

**FCFE-MIB**

See [Fibre Channel fabric element management information base](#).

**FCIA**

See [Fibre Channel Industry Association](#).

**FC IP**

See [Fibre Channel IP address](#).

**FCMGMT**

See [Fibre Channel management framework integration](#).

**FC-PH**

See [Fibre Channel physical and signaling interface](#).

**feature key**

A unique key to enable additional product features. This key is entered into the *Configure Feature Key* dialog box in the Element Manager application to activate optional hardware and software features. Upon purchasing a new feature, McDATA provides the feature key to the customer.

**fiber**

The fiber-optic cable made from thin strands of glass through which data in the form of light pulses is transmitted. It is used for high-speed transmissions over medium (200 m) to long (10 km) distances.

**fiber-optic cable**

*Synonym for optical cable.*

**fibres**

A generic Fibre Channel term used to cover all transmission media types specified in the Fibre Channel Physical Layer (FC-PH) standard such as optical fiber, copper twisted pair, and copper coaxial cable.

**Fibre Channel**

FC. Integrated set of standards recognized by American National Standards Institute (ANSI) which defines specific protocols for flexible information transfer. Logically, a point-to-point serial data channel, structured for high performance.

**Fibre Channel adapter**

FC adapter. See [host bus adapter](#).

**Fibre Channel address**

A 3-byte node port (N\_Port) identifier which is unique within the address domain of a fabric. Each port may choose its own identifier, or the identifier may be assigned automatically during fabric login.

**Fibre Channel arbitrated loop**

FC-AL. A high-speed (100 Mbps) connection which is a true loop technology where ports use arbitration to establish a point-to-point circuit. Data can be transferred in both directions simultaneously, achieving a nominal transfer rate between two products of 200 Mbps.

**Fibre Channel Association**

FCA. The FCA is a non-profit corporation consisting of over 150 members throughout the world. Its mission is to nurture and help develop the broadest market for Fibre Channel products through market development, education, standards monitoring, and fostering interoperability among members' products.

**Fibre Channel fabric element**

FCFE. Any product linked to a fabric.

**Fibre Channel fabric element management information base**

FCFE-MIB. A table of variables available to network management stations and resident on a switch or director. Through the simple network management protocol (SNMP) these pointers can be manipulated to monitor, control, and configure the switch or director.

**Fibre Channel Industry Association**

FCIA. A corporation consisting of over 100 computer industry-related companies. Its goal is to provide marketing support, exhibits, and tradeshows for its member companies. The FCIA complements activities of the various standards committees.

**Fibre Channel I/O controller**

FCC-IOC. In a director, the integrated controller on the control processor (CTP) card dedicated to the task of managing the embedded Fibre Channel port. In a director or switch, the FCC-IOC controls the embedded Fibre Channel port and configures the ports' application-specific integrated circuits (ASICs).

**Fibre Channel IP address**

FC IP. The default FC IP on a new switch is a temporary number divided by the switch's world-wide name (WWN). The system administrator needs to enter a valid IP address.

**Fibre Channel management framework integration**

FCMGMT. A standard defined by the Fibre Alliance to provide easy management for Fibre Channel-based products such as switches, hubs, and host-bus adapters.

**Fibre Channel physical and signaling interface**

FC-PH. The American National Standards Institute (ANSI) document that specifies the FC-0 (physical signaling), FC-1 (data encoding), and FC-2 (frame construct) layers of the Fibre Channel protocol (*D*).

**Fibre Channel protocol for SCSI (FCP)**

FCP defines a high-level Fibre Channel mapping layer (FC-4) that uses lower-level Fibre Channel (FC-PH) services to transmit SCSI command, data, and status information between a SCSI initiator and a SCSI target across the FC link using FC frame and sequence formats.

**Fibre Channel standard**

American National Standards Institute (ANSI) standard that provides a common, efficient data transport system that supports multiple protocols. The architecture integrates both channel and network technologies, and provides active, intelligent interconnection among products. All data transmission is isolated from the control protocol, allowing use of point-to-point, arbitrated loop, or switched fabric topologies to meet the needs of an application.

**Fibre Connection**

FICON. An IBM set of products and services introduced in 1999 that is based on the Fibre Channel Standard. FICON technology uses fiber-optic cables as the data transmission medium, and significantly improves I/O performance (including one Gbps bi-directional data transfer). FICON is designed to coexist with ESCON™ channels, and FICON-to-ESCON control unit connections are supported (*D*).

**fibre port module**

FPM. A 1 gigabit-per-second module that contains four generic ports (Deports).

**FICON**

See [Fibre Connection](#).

**FICON Management Server**

An optional feature that can be enabled on the director or switch or switch through the Element Manager application. When enabled, host control and management of the director or switch or switch is provided through an S/390 Parallel Enterprise or 2/390 Series Server attached to a director or switch or switch port.

**FICON management style**

The management style that is most useful when attaching to IBM S/390 Enterprise Servers. See also [open systems management style](#); [management style](#).

**field-replaceable unit**

FRU. Assembly removed and replaced in its entirety when any one of its components fails (*D*). See [active field-replaceable unit](#).

**file server**

A computer that stores data centrally for network users and manages access to that data.

**file transfer protocol**

FTP. A TCP/IP-based client/server protocol used to transfer files to and from a remote host. Does not perform any conversion or translation.

**firmware**

Embedded program code that resides and runs on, for example, directors, switches, and hubs.

**firewall**

A networking product that blocks unauthorized access to all or parts of a network.

**firewall zoning**

Hardware enforced access between F\_Ports enforced at the source port. The hardware verifies the destination port against the zone defined for the source port.

**firmware**

Embedded program code that resides and runs on, for example, directors, switches, and hubs.

**FLASH memory**

Reusable nonvolatile memory that is organized as segments for writing, and as bytes or words for reading. FLASH memory is faster than read-only memory, but slower than random access memory (*D*).

**FLOGI**

See [fabric login command](#).

**FL\_Port**

See [fabric loop port](#).

**FPM**

See [fibre port module](#).

**F\_Port**

See [fabric port](#).

**frame**

A variable-length packet of data that is transmitted in frame relay technology.

**FRU**

See [field-replaceable unit](#).

**FTP**

See [file transfer protocol](#).

**G****Gb/s**

Acronym for gigabits per second.

**gateway address**

(1) In transmission control protocol/Internet protocol (TCP/IP), a product that connects two systems that use the same or different protocols. (2) In TCP/IP, the address of a router to which a product sends frames destined for addresses not on the same physical network (for example, not on the same Ethernet) as the sender. The hexadecimal format for the gateway address is XXX.XXX.XXX.XXX.

**Gb**

See [gigabit](#).

**GB**

See [gigabyte](#).

**GbIC**

See [gigabit interface converter](#).

**Gbps**

Acronym for gigabits per second.

**GHz**

See [gigahertz](#).

**generic port**

G\_Port. Physical interface on a director or switch that can function either as a fabric port (F\_Port) or an expansion port (E\_Port), depending on the port type to which it connects. See *also* [bridge port](#); [expansion port](#); [fabric loop port](#); [fabric port](#); [hub port](#); [node loop port](#); [node port](#); [segmented expansion port](#).

**generic port module card**

GPM card. A port card that implements four generic ports (G\_Ports) and provides the physical connection point for links to Fibre Channel products.

**gigabit**

Gb. A unit of measure for data storage, equal to approximately 134,217,728 bytes. Approximately one eighth of a gigabyte.

**gigabit interface converter**

GbIC. A removable module that converts an electrical serial data stream to an optical or amplified electrical serial data stream. Contains connector for attaching fiber-optic cable.

**gigabyte**

GB. A unit of measure for data storage, equal to 1,073,741,824 bytes. Generally approximated as one billion bytes (D).

**gigahertz**

GHz. One billion cycles per second (Hertz) (D).

**GPM card**

See [generic port module card](#).

**G\_Port**

See [generic port](#).

**graphical user interface**

GUI. A visually oriented interface where the user interacts with representations of real-world objects displayed on the computer screen. Interactions with such objects produce actions that are intuitive to the user (D).

**GSM card**

A generic port (G\_Port) module card containing shortwave laser ports for multimode fiber-optic cables.

**GUI**

See [graphical user interface](#).

**H****H\_Port**

See [hub port](#).

**hard drive**

An electromechanical product used for information storage and retrieval, incorporating one or more rotating disks on which data is recorded, stored, and read magnetically.

**Hardware Log**

Director or switch *Hardware Log*. Log displayed through the Element Manager application that provides a history of FRU removals and replacements (insertions) for an individual director or switch. The information is useful to maintenance personnel for fault isolation and repair verification. See also [Audit Log](#); [master log](#); [Link Incident Log](#); [Threshold Alert Log](#).

**hardware**

Physical equipment (director, switch, or personal computer) as opposed to computer programs or software.

**hardware management console**

The console runs the Hardware Management console application (HWMCA), and is the operations and management personal computer (PC) platform for S/390 and z/Series servers.

**HBA**

See [host bus adapter](#).

**heterogeneous fabric**

A fabric containing open-fabric-compliant products from various vendors. *Contrast with* [homogeneous fabric](#).

**hexadecimal**

A numbering system with base of sixteen; valid numbers use the digits 0 through 9 and characters A through F, where A represents 10 and F represents 15 (D).

**homogeneous fabric**

A fabric consisting of only one vendor's products. *Contrast with* [heterogeneous fabric](#).

**hop**

(1) Data transfer from one node to another node. (2) Describes the number of switches that handle a data frame from its origination point through its destination point.

**hop count**

The number of hops a unit of information traverses in a fabric.

**host**

The computer that other computers and peripherals connect to.

**host bus adapter**

HBA. Logic card that provides a link between the server and storage subsystem, and that integrates the operating systems and I/O protocols to ensure interoperability.

**host group**

The collection of HBAs and NASs in a fabric discovered by the SAN Management application. Host groups display with a yellow background on the Physical Map.

**host processor**

(1) A processor that controls all or part of a user application network (T). (2) In a network, the processing unit in which resides the access method for the network (D).

**hot spare**

An extra disk that is currently running in the RAID, but is there for backup. If a working disk fails, its data can be reconstructed from the remaining disks and written to the hot spare.

**HTTP**

See [hypertext transport protocol](#).

**hub**

In Fibre Channel protocol, a product that connects nodes into a logical loop by using a physical star topology.

**hub port**

H\_Port. In arbitrated loop products, a port that uses arbitrated loop protocols. The physical interface that attaches to a loop product, either an end product or another loop interconnect product (hub).

**hyperlink**

A predefined link for jumping from one location to another, within the same computer or network site or even to a location at a completely different physical location. Commonly used on the world wide web for navigation, reference, and depth where published text does not suffice.

**hypertext transport protocol**

HTTP. A simple protocol that allows world wide web pages to be transferred quickly between web browsers and servers.

**I****ID**

See [identifier](#).

**identifier**

ID. (1) One or more characters used to identify or name a data element and possibly to indicate certain properties of that data element (*D*, *T*). (2) A sequence of bits or characters that identifies a program, device, or system to another program, device, or system. See also [port name](#).

**IEEE**

See [Institute of Electrical and Electronics Engineers](#).

**IML**

See [initial machine load](#).

**in-band**

Transmission of management protocol over the Fibre Channel transport. See also [out-of-band](#).

**in-band discovery**

The process through which the SAN Management application Server gathers data about the in-band data flow and LUNs from the HBA driver. The HBA driver must support the Fibre Alliance HBA API for in-band discovery to work properly. See also [out-of-band discovery](#).

**in-band management**

Management of the director or switch through Fibre Channel. An interface connection to a port card. Contrast with [out-of-band management](#).

**industry standard architecture**

ISA. Bus architecture designed for personal computers (PCs) that use an Intel 80386, 80486, or Pentium microprocessor. ISA buses are 32 bits wide and support multiprocessing.

**information message**

Message notifying a user that a function is performing normally or has completed normally. See also [error message](#); [warning message](#).

**information services**

IS. IS is the name of the department responsible for computers, networking, and data management. See also [information technology](#).

**information technology**

IT. The broad subject concerned with all aspects of managing and processing information, especially within a large organization or company. Because computers are central to information management, computer departments within companies and universities are often called IT departments. See also [information services](#).

**initial machine load**

IML. Hardware reset for all installed control processor (CTP) cards on the director or switch. This reset does not affect other hardware. It is initiated by pushing the IML button on a director's or switch's operating panel.

**initial program load**

IPL. The process of initializing the product and causing the operating system to start. An IPL may be initiated through a menu option or a hardware button.

**initial program load configuration**

IPL configuration. In FICON management style, information stored in a director or switch's nonvolatile memory that contains default configurations. The director or switch loads the file for operation when powered on.

**input/output**

I/O. (1) Pertaining to a device whose parts can perform an input process and an output process at the same time (*I*). (2) Pertaining to a functional unit or channel involved in an input process, output process, or both, concurrently or not, and to the data involved in such a process. (3) Pertaining to input, output, or both (*D*). (4) An operation or product that allows input and output.

**Institute of Electrical and Electronics Engineers**

IEEE. An organization of engineers and technical professionals that promotes the development and application of electronic technology and allied sciences.

**interface**

(1) A shared boundary between two functional units, defined by functional, signal, or other characteristics. The concept includes the specification of the connection of two products having different functions (*T*). (2) Hardware, software, or both, that link systems, programs, or products (*D*).

**Internet protocol**

IP. Network layer for the transmission control protocol/Internet protocol (TCP/IP) protocol used on Ethernet networks. IP provides packet routing, fragmentation, and reassembly through the data link layer (*D*).

**Internet protocol address**

IP address. Unique string of numbers (in the format xxx.xxx.xxx.xxx) that identifies a product on a network.

**interoperability**

Ability to communicate, execute programs, or transfer data between various functional units over a network.

**interoperability mode**

Interpol mode. A management style set through management software that allows products to operate in homogeneous or heterogeneous fabrics.

**interop mode**

See [interoperability mode](#).

**interrupt**

A signal sent by a subsystem to the central processing unit (CPU) that signifies a process has either completed or could not be completed.

**interswitch link**

ISL. Physical expansion port (E\_Port) connection between two directors in a fabric.

**intranet**

A private version of the Internet that provides a cost-effective way to publicize critical information and provide an interactive communication path for heterogeneous systems. Internal to a specific organizational structure and secured from or disconnected from the global Internet.

**I/O**

See [input/output](#).

**IOPS**

Input/output operations per second.

**IP**

See [Internet protocol](#).

**IP address**

See [Internet protocol address](#).

**IS**

See [information services](#).

**IPL**

See [initial program load](#).

**IPL configuration**

See [initial program load configuration](#).

**ISL**

See [interswitch link](#).

**ISL hop**

Interswitch link hop. See [hop](#).

**isolated E\_Port**

Isolated expansion port.

**isolated expansion port**

Isolated E\_Port.

**isolated group**

A collection of isolated devices not connected to the SAN but discovered by the SAN Management application. The isolated group displays with a gray background near the bottom of the Physical Map.

**IT**

See [information technology](#).

**J**

**Java**

An object-oriented programming language derived from C++ that produces code that is platform independent. Developed by Sun Microsystems designed for distribution and distributable applications development. Java applications require a program called the Java Virtual Machine (JVM) to execute. JVMs have been developed for many of the mainstream platforms and operating systems.

**JBOD**

See [just a bunch of disks](#).

**just a bunch of disks**

JBOD. Refers to a rack of disks without data redundancy or striping.

**K**

**Kb**

See [kilobit](#).

**KB**

See [kilobyte](#).

**kilobit**

Kb. A unit of measure for data storage, equaling 1,024 bits, or two to the tenth power. Kilobits are generally approximated as being one thousand bits.

**kilobyte**

KB. A unit of measure for data storage, equaling 1,024 bytes, or two to the tenth power. Kilobytes are generally approximated as being one thousand bytes.

**L****label**

A discovered or user-entered property value that displays below each product on the Physical Map, or topology.

**LAN**

See [local area network](#).

**laser**

Laser is an acronym for light amplification by stimulated emission of radiation. A product that produces a very powerful narrow beam of coherent light of a single wavelength by simulating the emissions of photons from atoms, molecules, or ions.

**latency**

Amount of time elapsed between receipt of a data transmission at a switch's incoming fabric port (F\_Port) from the originating node port (N\_Port) to retransmission of that data at the switch's outgoing F\_Port to the destination N\_Port. The amount of time it takes for data transmission to pass through a switching product. The time it takes for data to go from an HBA to a product's LUN and back to the HBA.

**LCD**

Liquid crystal display.

**light-emitting diode**

LED. A semiconductor chip that emits visible or infrared light when electricity passes through it. LEDs are used on switch or director field-replaceable units (FRUs) and the front bezel to provide visual indications of hardware status or malfunctions.

**LIN**

See [link incident](#).

**link**

Physical connection between two products on a switched fabric. A link consists of two conductors, one used for sending and the other for receiving, thereby providing a duplex communication path.

**link incident**

LIN. Interruption to link due to loss of light or other causes. See also [link incident alerts](#).

**link incident alerts**

A user notification, such as a graphic symbol in the Element Manager application *Hardware View* that indicates that a link incident has occurred. See also [link incident](#).

**Link Incident Log**

Director or switch *Link Incident Log*. Log displayed through the Element Manager application that provides a history of Fibre Channel link incidents (with associated port numbers) for an individual director or switch. The information is useful to maintenance personnel for isolating port problems (particularly expansion port (E\_Port) segmentation problems) and repair verification. See also [Audit Log](#); [master log](#); [Hardware Log](#); [Threshold Alert Log](#).

**LIP**

See [loop initialization primitive](#).

**load balancing**

Ability to evenly distribute traffic over multiple interswitch links within a fabric. Load balancing on *McDATA* or *IBM* directors and switches takes place automatically.

**local area network**

LAN. A computer network in a localized geographical area (for example, a building or campus), whose communications technology provides a high-bandwidth medium to which many nodes are connected (*D*). See also [metropolitan area network](#); [storage area network](#); [wide area network](#).

**logical port address**

In a director or switch, the address used to specify port connectivity parameters and to assign link addresses for the attached channels and control units.

**logical switch number**

LSN. A two-digit number used by the I/O configuration program (IOCP) to identify a director or switch (*D*).

**logical unit number**

LUN. In Fibre Channel addressing, a logical unit number is a number assigned to a storage product which, in combination with the storage product's node port's world-wide name, represents a unique identifier for a logical product on a storage area network. Peripherals use LUNs to represent addresses. A small computer system interface (SCSI) product's address can have up to eight LUNs.

**login server**

Entity within the Fibre Channel fabric that receives and responds to login requests.

**loop**

A loop is a configuration of products connected to the fabric via a fabric loop port (FL\_Port) interface card.

**loop address**

In Fibre Channel protocol, a term indicating the unique ID of a node in Fibre Channel loop topology, sometimes referred to as a loop ID.

**loop group**

A collection of SAN devices that are interconnected serially in a single loop circuit. Loop groups discovered by the SAN Management application display with a gray background on the Physical Map.

**loop initialization primitive**

LIP. In an arbitrated loop product, a process by which devices connected to hub ports (H\_Ports) on the arbitrated loop device notify other devices and the switch of the presence in the loop by sending LIP sequences and subsequent frames through the loop. This process allows linked arbitrated loop devices to perform fabric loop port (FL\_Port) arbitration as they link through hub ports.

**loop master**

In an arbitrated loop device, a reference to the loop master World Wide Name (WWN) field in the *Loop View*, the loop master is the arbitrated loop device that is responsible for allocating arbitrated loop physical addresses (AL-PAs) on the loop. An arbitrated loop device becomes the loop master through arbitration when there are multiple arbitrated loop devices on the loop. The arbitrated loop device with the lowest WWN becomes the loop master.

**loop switches**

Loop switches support node loop port (NL\_Port) Fibre Channel protocols. Switches sold as loop support but upgradeable to fabric switches recounted as loop switches.

**loop port**

L\_Port. *Synonym for* [hub port](#).

**loopback plug**

In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input. *Synonymous with* [wrap plug](#).

**loopback test**

Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.

**L\_Port**

Loop port. *Synonym for* [hub port](#).

**LSN**

See [logical switch number](#).

**LUN**

See [logical unit number](#).

**M****MAC address**

See [media access control address](#).

**mainframe**

A powerful multi-user computer capable of supporting many hundreds or thousands of users simultaneously.

**MAN**

See [metropolitan area network](#).

**maintenance port**

Connector on the director or switch where a PC running an American National Standard Code for Information Interchange (ASCII) terminal emulator can be attached or dial-up connection made for specialized maintenance support.

**managed product**

Hardware product that can be managed with the Element Manager application. *McDATA* or directors and switches are managed products. See also [device](#).

**management information base**

MIB. Related set of software objects (variables) containing information about a managed device and accessed via simple network management protocol (SNMP) from a network management station.

**management session**

A session that exists when a user logs on to your SAN management application. Your SAN management application can support multiple concurrent management sessions. The user must specify the network address of your SAN management application's server at logon time.

**management style**

In directors or switches, in managed products, a selection between FICON and open systems management style. See *also* [open systems management style](#); [FICON management style](#).

**manager**

A SAN management application.

**master log**

Record of significant events that have occurred on the SAN, including configuration and discovery events.

**Mb**

Megabit.

**MB**

See [megabyte](#).

**Mbps**

Megabits per second.

**MBps**

Megabytes per second.

**media access control address**

MAC address. Hardware address of a node (device) connected to a network.

**megabyte**

MB. A unit of measure for data storage, equal to 1,048,576 bytes. Generally approximated as one million bytes.

**memory**

A device or storage system capable of storing and retrieving data.

**menu**

A list of items displayed on a monitor from which a user can make a selection.

**menu bar**

The menu bar is located across the top of a window. Pull-down menus are displayed by clicking on the menu bar option with the mouse, or by pressing **ALT** with the underlined letter of the name for the menu bar option (*D*).

**message path controller card**

MPC card. In the ED-5000 Director, a card that provides the mechanism for messages to be sent and received between ports on the director. The card also provides a system clock source, and central control and distribution of clocks for MPC, G\_Port module (GPM), and central memory module (CMM) cards. See *also* [Fibre Channel I/O controller](#).

**metropolitan area network**

MAN. A network capable of high-speed communications over distances up to about 100 kilometers. See *also* [local area network](#); [storage area network](#); [wide area network](#).

**MIB**

See [management information base](#).

**microsecond**

μs.

**mirroring**

The writing of data to pairs of drives in an array, creating two exact copies of the drive contents. This procedure provides a backup of data in case of a failure.

**model**

The model identification assigned to a device by its manufacturer.

**modem**

Modem is an abbreviation for modulator/demodulator. A communication device that converts digital computer data to signals and signals to computer data. These signals can be received or transmitted by the modem via a phone line or other method of telecommunication.

**ms**

Millisecond.

**multimedia**

A simultaneous presentation of data in more than one form, such as by means of both visual and audio.

**multiswitch fabric**

Fibre Channel fabric created by linking more than one director or fabric switching device within a fabric.

## N

**name server**

(1) In TCP/IP, see [domain name server](#). (2) In Fibre Channel protocol, a server that allows node ports (N\_Ports) to register information about themselves. This information allows N\_Ports to discover and learn about each other by sending queries to the name server.

**name server zoning**

Node port (N\_Port) access management that allows N\_Ports to communicate if and only if they belong to a common name server zone.

**NAS**

See [network-attached storage](#).

**network**

An arrangement of hardware, software, nodes, and connecting branches that comprises a data communication system. The International Organization for Standardization (ISO) seven-layer specification partitions a computer network into independent modules from the lowest (physical) layer to the highest (application) layer (D).

**network address**

Name or address that identifies a device on a transmission control protocol/Internet protocol (TCP/IP) network. The network address can be either an IP address in dotted-decimal notation (composed of four three-digit octets in the format xxx.xxx.xxx.xxx) or a domain name (as administered on a customer network).

**network-attached storage**

NAS. Storage connected directly to the network, through a processor and its own operating system. Lacks the processor power to run centralized, shared applications.

**network interface card**

NIC. An expansion board inserted into a computer so the computer can be connected to a network. Most NICs are designed for specific types of networks, protocols, and medias, although some can serve multiple networks.

**network management**

The broad subject of managing computer networks. There exists a wide variety of software and hardware products that help network system administrators manage a network. Network management covers a wide area, including security, performance, and reliability.

**never principal**

The setting that prevents the product from becoming the principal switch for a fabric.

**nickname**

Alternate name assigned to a world-wide name for a node, director or switch in the fabric.

**NL\_Port**

See [node loop port](#).

**node**

In Fibre Channel protocol, an end device (server or storage device) that is or can be connected to a switched fabric. See *also* [device](#).

**node loop port**

NL\_Port. A physical interface within an end device (node) that participates in a loop containing one or more fabric loop ports (FL\_Ports) or other NL\_Ports. See *also* [expansion port](#); [fabric loop port](#); [fabric port](#); [hub port](#); [node port](#).

**node port**

N\_Port. Physical interface within an end device that can connect to an fabric port (F\_Port) on a switched fabric or directly to another N\_Port (in point-to-point communications). See *also* [expansion port](#); [fabric loop port](#); [fabric port](#); [hub port](#); [node loop port](#).

**node port identifier**

N\_Port ID. In Fibre Channel protocol, a unique address identifier by which an N\_Port is uniquely known. It consists of a domain (most significant byte), an area, and a port, each 1 byte long. The N\_Port ID is used in the source identifier (S\_ID) and destination identifier (D\_ID) fields of a Fibre Channel frame.

**nonvolatile random access memory**

NV-RAM. RAM that retains its content when the device power is turned off.

**N\_Port**

See [node port](#).

**N\_Port ID**

See [node port identifier](#).

**NV-RAM**

See [nonvolatile random access memory](#).

**O****octet**

An 8-bit quantity, often called a byte or word. An octet can equal a byte as long as the byte equals eight bits. See [also byte](#).

**OEM**

See [original equipment manufacturer](#).

**offline**

Referring to data stored on a medium, such as tape or even paper, that is not available immediately to the user.

**offline sequence**

OLS. (1) Sequence sent by the transmitting port to indicate that it is attempting to initialize a link and has detected a problem in doing so. (2) Sequence sent by the transmitting port to indicate that it is offline.

**offline state**

When the switch or director is in the offline state, all the installed ports are offline. The ports transmit an offline sequence (OLS) and they cannot accept a login got connection from an attached device. *Contrast with* [online state](#).

**OLS**

See [offline sequence](#).

**online**

Referring to data stored on the system so it is available immediately to the user.

**online diagnostics**

Diagnostics that can be run by the customer engineer while the operational software is running. These diagnostics do not impact user operations.

**online state**

When the switch or director is in the online state, all of the unblocked ports are allowed to log in to the fabric and begin communicating. Devices can connect to the switch or director if the port is not blocked and can communicate with another attached device if both devices are in the same zone, or if the default zone is enabled. *Contrast with* [offline state](#).

**Open Systems Architecture**

OSI. A model that represents a network as a hierarchical structure of functional layers. Each layer provides a set of functions that can be accessed and used by the layer above. Layers are independent, in that implementation of a layer can be changed without affecting other layers (*D*).

**open systems management server**

OSMS. An optional feature that can be enabled on the director or switch through the Element Manager application. When enabled, host control and management of the director or switch are provided through an Open System Interconnection (OSI) device attached to a director or switch port.

**open systems management style**

The mode that is used for open fabrics. See also [management style](#); [FICON management style](#).

**operating system**

OS. Software that controls execution of applications and provides services such as resource allocation, scheduling, I/O control, and data management. Most operating systems are predominantly software, but partial hardware implementations are possible (*D*, *T*).

**Operating System/390**

OS/390™. An integrated, open-enterprise server operating system developed by IBM that incorporates a leading-edge and open communications server, distributed data and file services, parallel Sysplex™ support, object-oriented programming, distributed computing environment, and open application interfaces (*D*).

**original equipment manufacturer**

OEM. A company that has a special relationship with computer producers. OEMs buy components and customize them for a particular application. They sell the customized computer under their own name. OEMs may not actually be the original manufacturers. They usually customize and market the product.

## OS

See [operating system](#).

## OS/390™

See [Operating System/390](#).

## OSI

See [Open Systems Architecture](#).

## OSMS

See [open systems management server](#).

## out-of-band

Transmission of management protocols outside of the Fibre Channel network, typically over Ethernet. See also [in-band](#).

## out-of-band discovery

The process through which the SAN Management application connects to the switches via the IP network. Device information is copied from the SNMP server to the Server. See also [in-band discovery](#).

## out-of-band management

Transmission of management information, using frequencies or channels other than those routinely used for information transfer.

## P

### packet

In Fibre Channel protocol, Logical unit of information (usually in the form of a data frame) transmitted on a network. It contains a header (with all relevant addressing and timing information), the actual data, and a trailer (which contains the error checking function, usually in the form of a cyclic redundancy check), and frequently user data.

### panel

A logical component of the interface window. Typically, a heading and/or frame marks the panel as an individual entity of the window. Size and shape of the panel and its data depend upon the purpose of the panel and may or may not be modified.

### partition

A way to logically divide a hard drive so that an operating system treats each partition as a separate hard drive. Each partition has a unique drive letter.

## PC

See [personal computer](#).

## persistent binding

A form of server-level access control that uses configuration information to bind a server to a specific Fibre Channel storage volume (or logical device), using a unit number. See also [access control](#).

## personal computer

PC. A portable computer that consists of a system unit, display, keyboard, mouse, one or more diskette drives, and internal fixed-disk storage (D).

## physical map

The map of the topology that displays when you select the View tab on the main window of the SAN Management application. The Physical Map displays devices and their connections and ports.

## point-to-point

A Fibre Channel protocol topology that provides a single, direct connection between two communication ports. The director or switch supports only point-to-point topology (D). See also [arbitrated loop](#).

## polling delay

The time in seconds between successive discovery processes during which discovery is inactive.

## port

Receptacle on a device to which a cable leading to another device can be attached. Ports provide Fibre Channel connections (D).

## port address name

A user-defined symbolic name of 24 characters or less that identifies a particular port address.

## port authorization

Feature of the password definition function that allows an administrator to extend operator-level passwords to specific port addresses for each director or switch definition managed by a personal computer (PC). Port authorization affects only operator-level actions for active and saved matrices (D).

## port card

Field-replaceable hardware component that provides the port connections for fiber cables and performs specific device-dependent logic functions.

**port card map**

Map showing port numbers and port card slot numbers inside a hardware cabinet.

**port name**

Name that the user assigns to a particular port through the Element Manager application. See also [identifier](#).  
*Synonymous with* [address name](#).

**POST**

See [power-on self-test](#).

**power-on self-test**

POST. Series of diagnostic tests that are run automatically by a device when the power is turned on

**preferred domain ID**

Configured value that a switch requests from the Principal Switch. If the preferred value is already in use, the Principal Switch assigns a different value.

**principal switch**

In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.

**private device**

A loop device that cannot transmit a fabric login command (FLOGI) command to a switch or director, nor communicate with fabric-attached devices. *Contrast with* [public device](#).

**private loop**

A freestanding Arbitrated Loop with no fabric attachment.

**product list**

The list of SAN products, groups, and ports, which displays on the left-hand side of the main window in the application.

**product name**

User-configurable identifier assigned to a managed product. Typically, this name is stored on the product itself. A director or switch product name can also be accessed by a simple network management protocol (SNMP) manager as the system name.

**prohibited port connection**

In a director or switch, in FICON management style, an attribute that removes dynamic connectivity capability.

**protocol**

(1) Set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) In systems network architecture, the meanings of and sequencing rules for requests and responses for managing the network, transferring data, and synchronizing network component states. (3) A specification for the format and relative timing of data exchanged between communicating devices (*D, I*).

**public device**

A loop device that can transmit a fabric login command (FLOGI) to a switch, receive acknowledgement from the switch's login server, register with the switch's name server, and communicate with fabric-attached devices. Public devices communicate with fabric-attached devices through the switch's bridge port (B\_Port) connection to a director or switch. *Contrast with* [private device](#).

**public loop**

A public loop is connected to a switched fabric (through the switch bridge port (B\_Port)), and the switch has an active embedded fabric loop port (FL\_Port) that is user transparent. All devices attached to the loop can communicate with each other, and public devices attached to the loop can communicate with fabric-attached devices.

**pull-down menu**

See [drop-down menu](#).

**R****RAID**

See [redundant array of independent disks](#).

**RAM**

See [random access memory](#).

**R\_A\_TOV**

See [resource allocation time-out value](#).

**random access memory**

RAM. A group of computer memory locations that is numerically identified to allow high-speed access by the controlling microprocessor. A memory location is randomly accessed by referring to its numerical identifier (*D*). *Contrast with* [read-only memory](#).

**read-only memory**

ROM. An information storage chip with permanent memory. Stored information cannot be changed or deleted except under special circumstances (D). *Contrast with [random access memory](#).*

**redundancy**

Performance characteristic of a system or product whose integral components are backed up by identical components to which operations automatically failover in the event of a component failure. Redundancy is a vital characteristic of virtually all high-availability (24 hours/7 days per week) computer systems and networks.

**redundant array of independent disks**

RAID. Grouping of hard drives in a single system to provide greater performance and data integrity. RAID systems have features that ensure data stored on the drives are safe and quickly retrievable.

**remote computer running client software**

Workstation, such as a personal computer (PC) or UNIX workstation, running SAN management and Element Manager client application software that can access the server platform over a local area network (LAN) connection.

**remote notification**

See [event notification](#).

**resource allocation time-out value**

R\_A\_TOV. R\_A\_TOV is a value used to time-out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered.

**right-click menu**

See [shortcut menu](#).

**ROM**

See [read-only memory](#). *Contrast with [random access memory](#).*

**router**

An attaching device that connects two local area network (LAN) segments, which use similar or different architectures, at the reference model network layer (D). *Contrast with [bridge](#).*

**S**

**SAN**

See [storage area network](#).

**EFCM Basic interface**

The interface provides a graphical user interface (GUI) similar to the Element Manager application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through an embedded web server interface.

**SA OS/390™**

See [System Automation for Operating System/390](#).

**SBAR**

See [serial crossbar assembly](#).

**segment**

A fabric segments when one or more switches cannot join the fabric because of various reasons. The switch or switches remain as separate fabrics.

**segmented E\_Port**

See [segmented expansion port](#).

**segmented expansion port**

Segmented E\_Port. E\_Port that has ceased to function as an E\_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins. See *also* [bridge port](#); [fabric loop port](#); [fabric port](#); [generic port](#); [hub port](#); [node loop port](#); [node port](#).

**segmented loop port**

Allows you to divide a Fibre Channel private loop into multiple segments. Each segment can pass frames around as an independent loop and can connect through the fabric to other segments of the same loop.

**serial crossbar assembly**

SBAR. The assembly is responsible for Fibre Channel frame transmission from any director or switch port to any other director or switch port. Connections are established without software intervention.

**serial port**

A full-duplex channel that sends and receives data at the same time. It consists of three wires: two that move data one bit at a time in opposite directions, and a third wire that is a common signal ground wire.

**server**

A computer that provides shared resources, such as files and printers, to the network. Used primarily to store data, providing access to shared resources. Usually contains a network operating system.

**Server**

The computer that is hosting the SAN Management application. Multiple client systems can log in to the server to utilize the SAN Management application.

**server/device events**

Events occurring on the server or a designated device that meet criteria set by the user.

**Server Platform**

A server platform shipped with the product or supplied by the customer for the purpose of running the SAN management and Element Manager server applications.

**SFP transceivers**

See [small form factor pluggable transceivers](#).

**shared mode**

If a director or switch is in shared mode, all devices on the loop share the 100MB bandwidth available on the loop. In shared mode, only one end device can communicate with another device through the fabric loop port (FL\_Port) on the director or switch.

**shortcut menu**

The menu that displays when you right-click an icon or the background.

**simple mail transfer protocol**

SMTP. A transmission control protocol/Internet protocol (TCP/IP) protocol that allows the user to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents, or stores the mail.

**simple network management protocol**

SNMP. A transmission control protocol/Internet protocol (TCP/IP)-derived protocol governing network management and monitoring of network devices.

**simple network management protocol community**

SNMP community. Also known as SNMP community string. SNMP community is a cluster of managed products (in SNMP terminology, hosts) to which the server or managed product running the SNMP agent belongs.

**simple network management protocol community name**

SNMP community name. The name assigned to a given SNMP community. Queries from an SNMP management station to a device running an SNMP agent only elicit a response if those queries are addressed with the correct SNMP community name.

**simple network management protocol management station**

SNMP management station. An SNMP workstation personal computer (PC) used to oversee the SNMP network.

**SL\_Port**

See [segmented loop port](#).

**small form factor pluggable transceivers**

SFP transceivers. Laser-based optical transceivers for a wide range of networking applications requiring high data rates. The transceivers, which are designed for increased densities, performance, and reduced power, are well-suited for Fibre Channel applications.

**SMTP**

See [simple mail transfer protocol](#).

**SNMP**

See [simple network management protocol](#).

**SNMP community**

See [simple network management protocol community](#).

**SNMP community name**

See [simple network management protocol community name](#).

**SNMP management station**

See [simple network management protocol management station](#).

**SNMP time-out**

The maximum amount of time the SAN Management application waits for a device to respond to a request. The specified time applies to one retry only.

### **SNMP trap events**

SNMP is based on a manager/agent model. SNMP includes a limited set of management commands and responses. The management system issues messages telling an agent to retrieve various object variables. The managed agent sends a Response message to the management system. That message is an event notification, called a trap, that identifies conditions, such as thresholds, that exceed a predetermined value.

### **state**

The state of the switch or director. Possible values include online, offline, testing, and faulty. See [offline state](#); [online state](#).

### **static random access memory**

SRAM. SRAM is microprocessor-cache random access memory. It is built internal to the microprocessor or on external chips. SRAM is fast, but relatively expensive (*D*). Contrast with [dynamic random access memory](#).

### **storage area network**

SAN. A high-performance data communications environment that interconnects computing and storage resources so that the resources can be effectively shared and consolidated. See also [local area network](#); [metropolitan area network](#); [wide area network](#).

### **stored addresses**

In FICON management style, a method for configuring addresses.

### **subnet**

A portion of a network that shares a common address component. On transmission control protocol/Internet protocol (TCP/IP) networks, subnets are defined as all devices whose IP addresses have the same prefix. Dividing a network into subnets is useful for both security and performance reasons. IP networks are divided using a subnet mask.

### **subnet mask**

A mask used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

### **switch**

A device that connects, filters and forwards packets between local area network (LAN) segments or storage area network (SAN) nodes or devices.

### **switch group**

A switch and the collection of devices connected to it that are not in other groups. Switch groups discovered by the SAN Management application display with a gray background on the Physical Map.

### **switched mode**

If the arbitrated loop device is in switched mode, each pair of communicating ports on the arbitrated loop device can share the 100MB bandwidth. In switched mode, up to three pairs of loop devices can communicate with each other simultaneously. Or, a public device on the loop can communicate with another device on the fabric while up to two pairs of loop devices can communicate simultaneously.

### **switchover**

Changing a backup field-replaceable unit (FRU) to the active state, and the active FRU to the backup state.

### **switch priority**

Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric's principal switch. Lower values indicate higher likelihood of becoming the principal switch. A value of 1 indicates the highest priority; 225 is the lowest priority. A value of 225 indicates that the switch is not capable of acting as the principal switch. The value 0 is illegal.

### **System Automation for Operating System/390**

SA OS/390™. IBM licensed software that provides System/390 Parallel Sysplex™ management, automation capabilities, and integrated systems and network management. SA OS/390 manages host, remote processor, and I/O operations. SA OS/390 integrates the functions of Automated Operations Control for Multiple Virtual Storage (MVS™), ESCON™ Manager, and Target System Control Facility (*D*).

## **T**

### **TB**

See [terabyte](#).

**TCP/IP**

See [transmission control protocol/Internet protocol](#).

**technical support**

Single point of contact for a customer when assistance is needed in managing or troubleshooting a product. Technical support provides assistance 24 hours a day, seven days a week, including holidays. The technical support number is (877) 948-4448. *Synonymous with* [customer support](#).

**telnet**

The Internet standard protocol for remote terminal connection over a network connection.

**terabyte**

TB. One thousand (1,000) gigabytes; one terabyte of text on paper would consume 42,500 trees. At 12 characters per inch, 1 TB of data in a straight line would encircle the earth 56 times and stretch some 1.4 million miles equalling nearly three round trips from the earth to the moon.

**text box**

A box in a dialog box into which you can type data.

**Threshold Alert Log**

Director or switch *Threshold Alert Log*. Log displayed through the Element Manager application that provides details of threshold alert notifications for an individual director or switch. The log displays the date and time an alert occurred, and displays details about the alert as configured for the product. The information is useful to maintenance personnel for fault isolation and repair verification. See also [Audit Log](#); [master log](#); [Hardware Log](#); [Link Incident Log](#).

**TL\_Port**

See [translated loop port](#).

**topology**

Logical and/or physical arrangement of devices on a network.

**transfer rate**

The speed with which data can be transmitted from one device to another. Data rates are often measures in megabits (Mbps) or megabytes (MBps) per second, or gigabits (Gbps) or gigabytes per second (GBps).

**transmission control protocol/Internet protocol**

TCP/IP. A layered set of protocols (network and transport) that allows sharing of applications among devices on a high-speed local area network (LAN) communication environment (*D*). See also [Internet protocol](#).

**trap**

Unsolicited notification of an event originating from a simple network management protocol (SNMP) managed device and directed to an SNMP network management station.

**trap host**

Simple network management protocol (SNMP) management workstation that is configured to receive traps.

**translated loop port**

Connects to a private loop and allows connectivity between the private loop devices and “off loop” devices (devices not connected to that particular TL\_Port).

**trap recipient**

Receiver of a forwarded SNMP trap. Specifically, a trap receiver is defined by an IP address and port to which traps are sent. Presumably, the actual recipient is a software application running at the IP address and listening to the port.

**trap recipient**

In simple network management protocol (SNMP), Receiver of a forwarded SNMP trap. Specifically, a trap receiver is defined by an IP address and port to which traps are sent. Presumably, the actual recipient is a software application running at the IP address and listening to the port.

**U****UDP**

See [user datagram protocol](#).

**unblocked connection**

In a director or switch, the absence of the blocked attribute for a specific port. *Contrast with* [blocked connection](#). See [connectivity attribute](#). See also [allowed connection](#); [dynamic connection](#); [dynamic connectivity](#).

**unblocked port**

Devices communicating with an unblocked port can login to the director or switch and communicate with devices attached to any other unblocked port (assuming that this is supported by the current zoning configuration).

**uniform resource locator**

URL. A URL is the address of a document or other resource on the Internet.

**universal port module**

UPM. A flexible 1 gigabit-per-second or 2 gigabit-per-second module that contains four generic ports (G\_Ports).

**UNIX**

A popular multi-user, multitasking operating system originally designed to be a small, flexible system used exclusively by programmers. UNIX was one of the first operating systems to be written in a high-level programming language, namely C. This meant that it could be installed on virtually any computer for which a C compiler existed. Due to its portability, flexibility, and power, UNIX has become the leading operating system for workstations. Historically, it has been less popular in the personal computer market, but the emergence of a new version called Linux is revitalizing UNIX across all platforms.

**UPM**

See [universal port module](#).

**upper level protocol**

ULP. Protocols that map to and run on top of the Fibre Channel FC-4 layer. ULPs include Internet protocol (IP) and small computer system interface (SCSI) (D).

**URL**

See [uniform resource locator](#).

**user action events**

Actions taken by the user (for example, changes in the SAN, changed settings, etc.). Each such action is considered a user action event.

**user datagram protocol**

UDP. A connectionless protocol that runs on top of Internet protocol (IP) networks. User datagram protocol/Internet protocol (UDP/IP) offers very few error recovery services, instead providing a direct way to send and receive datagrams over an IP network. UDP/IP is primarily used for broadcasting messages over an entire network.

**V****vendor**

Developer or manufacturer of software or hardware.

**virtual machine**

VM®. (1) A virtual data processing system that appears to be at the exclusive disposal of a single user, but whose functions are accomplished by sharing the resources of a real data processing system. (2) A functional simulation of a computer system and its associated devices, multiples of which can be controlled concurrently by one operating system (D, T).

**VM®**

See [virtual machine](#).

**W****WAN**

See [wide area network](#).

**warning message**

A message that indicates a possible error has been detected. See also [error message](#); [information message](#).

**web server interface**

The interface provides a graphical user interface (GUI) similar to the Element Manager application, and supports director or switch configuration, statistics monitoring, and basic operations. With director or switch firmware installed, administrators or operators with a browser-capable personal computer (PC) and an Internet connection can monitor and manage the director or switch through a web server interface.

**wide area network**

WAN. A network capable of transmission over large geographic areas that uses transmission lines provided by a common-carrier. See also [local area network](#); [metropolitan area network](#); [storage area network](#).

**window**

The main window for the SAN Management application. All management and monitoring functions are performed through the SAN Management application window.

**Windows**

A graphical user interface and windowing system introduced by Microsoft Corporation in 1985. Windows runs on top of the MS-DOS operating system (D).

**workstation**

A terminal or microcomputer usually connected to a network or mainframe at which a user can perform applications.

**world-wide names**

WWN. Eight-byte string that uniquely identifies a Fibre Channel entity (that is, a port, a node, a switch, a fabric), even on global networks.

**wrap plug**

Synonym for [loopback plug](#).

**wrap test**

A test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input. A wrap test can transmit a specific character pattern through a system and compare the pattern received with the pattern transmitted (D).

**write authorization**

Permission for an simple network management protocol (SNMP) management station with the proper community name to modify writable management information base (MIB) variables.

**WWN**

See [world-wide names](#).

**X****XDF**

See [extended distance feature](#).

**Z****zip drive**

A high capacity floppy disk and disk drive developed by the Iomega Corporation. Zip disks are slightly larger than conventional floppy disks. The storage capacity for zip disks is between 100 and 250 MB of data. The zip drive and disk is used for backing up the laptop Management Server and is located on the communications tray behind the server platform.

**zone**

Set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can see each other. Those devices that occupy different zones cannot. See *also* [active zone set](#); [zone set](#); [zoning](#).

**zone library**

Zoning data that includes zones and zone sets for a fabric.

**zone member**

Specification of a device to be included in a zone. A zone member can be identified by the port number of the director or switch to which it is attached or by its port world-wide name (WWN). In multiswitch fabrics, identification of end-devices or nodes by WWN is preferable.

**zone set**

A collection of zones that may be activated as a unit. See *also* [active zone set](#); [zone](#).

**zoning**

Grouping of several devices by function or by location. All devices connected to a connectivity product, such as the director or switch, may be configured into one or more zones.



# Index

---

## A

- access
  - assigning, 90
  - changing, 91
  - removing, 91
- access levels
  - defined, 285
  - user groups, 285
- activating discovery, 141
- active session management feature, 285
- active sessions, viewing, 101
- ADAPTER table, for MySQL, 257
- add/delete properties feature, 285
- adding
  - community strings, 212
  - device shortcut menu option, 126
  - IP addresses, 142
  - servers, 75, 78
  - tool, 123
  - Tools menu option, 124
  - trap recipients, 198
  - users, 90
- adding trap recipients, 209, 211
- adding users to groups, 98
- admin access, assigning, 90, 91
- administrator access, defined, 285
- AIX
  - uninstalling from, 22
- alerts, clearing ISL alerts, 196
- applications, opening, 129
- applications, opening from the application, 123
- ASM switch icon, 244
- assigning users to groups, 98
- associating HBAs to servers, 77
- attention, products needing, 164
- audit log
  - copying from, 219
  - overview, 216

## B

- B model products, managing, M model products, managing, 128
- back up and restore
  - rack-mount unit, 26, 34
- backup feature, 285
- blade switch icon, 244
- bridge group icon, 245
- bridge icon, 244
- browse access, assigning, 90, 91

## C

- call home event notification feature, 285
- call home status, determining, 69
- changing
  - device's shortcut menu, 127
  - fabric properties, 166
  - IP addresses, 144
  - nicknames of fabrics, 166
  - product properties, 163
  - product types, 163
  - TCP/IP ports, 242
  - Tools menu, 125
  - user accounts, 91
  - users, 91
  - view options, 103
- changing TCP/IP ports, 214
- clearing
  - events, 217
- clearing ISL alerts, 196
- community strings
  - adding, 212
  - configuring, 147
  - editing, 213
  - removing, 213
  - reverting to default, 149
- compatibility, with applications, 242
- Configure menu, 64

- configuring
  - community strings, 147
  - discovery, 139
  - event notification
    - e-mail, 220
  - remote access, 100
  - trap forwarding, 197
- CONNECTION table, for MySQL, 257
- connections
  - on persisted fabrics, 196
  - status, determining, 68
- copying from logs, 219
- counting frames, overview, 199
- creating user groups, 94
- creating, user accounts, 90

## D

- data
  - exporting, 109
  - importing, 109
- database
  - exporting to, 113
  - setting up
    - DB2, 115
    - MySQL, 115
- DB2 database
  - setting up, 115
- deactivating discovery, 141
- default community strings, 149
- degraded icon, 246
- deleting
  - reports, 227
  - users, 91
- deleting servers, 78
- deleting Tools menu options, 125
- deleting users from groups, 99
- determining users, 89
- device administration feature, 285
- device icons, 243
- device maintenance feature, 285
- device operation feature, 285
- DEVICE table, for MySQL, 258
- device tips, turning on and off, 104
- device's shortcut menu
  - adding option to, 126
  - editing, 127
  - removing option from, 127
- devices, finding in persisted fabrics, 197

- director icon, 243, 244
- Discover menu, 63
- discover on/off feature, 285
- discovery
  - configuring, 139
  - in-band, 132
  - in-band, enabling, 139
  - issues, 231
  - out-of-band, 132
  - out-of-band, enabling, 139
  - overview, 131, 132
  - setting up, 139
  - turning on and off, 141, 151
- discovery setup feature, 285
- disk, exporting to, 109
- documentation, where to find, 235

## E

- Edit menu, 60
- editing
  - community strings, 213
- editing trap recipients, 210
- editing user groups, 96
- editing, device's shortcut menu, 127
- EFCM
  - installing, 13
  - starting, 23
  - uninstalling, 21
- Element Manager session, launching, 128
- element manager, opening, 162
- e-mail event notification setup feature, 285
- e-mail notification, configuring, 220
- e-mail, exporting to, 109
- enclosure group icon, 245
- enterprise fabric mode
  - configuring, 175
  - overview, 174
- enterprise fabric mode feature, 285
- ethernet events, enabling, 222
- event log
  - copying from, 219
  - overview, 58, 216
- event management feature, 285
- event notification
  - configuring, 222
  - e-mail, 220
  - overview, 220

## events

- clearing, 217
- copying, 219
- exporting, 217
- filtering, 92, 218
- icons, 246
- monitoring, 216
- viewing, 216

export feature, 285

## exporting

- events, 217
- files, 109
- overview, 109
- setting up DB2 database, 115
- setting up MySQL database, 115

# F

## fabric binding

- adding detached devices, 180
- adding switches, 179
- disabling, 179
- enabling, 178
- overview, 176
- removing switches, 181

fabric binding feature, 285

fabric group icon, 245

FABRIC table, for MySQL, 258, 260, 262, 263, 266, 269

## fabrics

- changing nicknames for, 166
- changing properties, 166
- determining status, 68
- determining status of, 166
- persisted, determining status, 195
- persisting, 194
- unpersisting, 194
- unpersisting product, 194
- viewing, 218

failed icon, 246

FCIP bridge group icon, 245

FCIP bridge icon, 244

FCIP gateway group icon, 245

FCIP gateway icon, 244

## feature

- active session management, 285
- add/delete properties, 285
- backup, 285
- call home event notification, 285
- device administration, 285
- device maintenance, 285
- device operation, 285
- discover on/off, 285
- discovery setup, 285
- e-mail event notification setup, 285
- enterprise fabric mode, 285
- event management, 285
- export, 285
- fabric binding, 285
- frame sniffer, 285
- group manager-create event log, 285
- group manager-firmware install, 285
- group manager-run data collection, 285
- import, 285
- license update, 285
- log management, 285
- LUN management, 285
- map editing, 285
- map HBA to server, 285
- map loop to hub, 285
- map port to storage, 285
- monitor ethernet event, 286
- performance, 286
- persist fabric, 286
- planning, 286
- port fencing, 286
- properties edit, 286
- remote access, 286
- report, 286
- security admin, 286
- setup tools, 286
- show route, 286
- shutdown, 286
- SNMP agent configuration, 286
- software configuration properties, 286
- trap forwarding, 286
- user management, 286
- view management, 286
- virtual fabric, 286

feature documentation, 235

## files

- exporting, 109
- importing, 109, 116

## filtering events

- in master log, 218
- per user, 92

- finding
  - products, 163
  - topics in help, 52
- finding users, 99
- firewall configuration
  - forcing port in RMI registry, 253
  - forcing server and client port number, 253
  - TCP port numbers for RMI, 252
- flyovers, turning on and off, 104
- frame sniffer
  - configuring, 199
  - events in log, 199
  - refreshing, 206
  - session
    - deleting, 205
    - stopping, 203
  - test
    - adding, 201
    - deleting, 205
    - editing, 204
    - running, 202
    - stopping, 203
- frame sniffer feature, 285

## G

- generating reports, 224
- generating router reports, 227
- generating zone library reports, 228
- ghost products, finding corresponding real products, 197
- group manager-create event log feature, 285
- group manager-firmware install feature, 285
- group manager-run data collection feature, 285
- groups
  - assigning users, 98
  - creating for users, 94
  - determining, 99
  - editing for users, 96
  - finding users in, 99
  - removing users, 99
- groups, icons, 245

## H

- HBAs
  - associating to servers, 77
  - unassociating, 77
- Help menu, 66
- hide routes, overview, 166
- HISTORICALPERFORMANCE table, for MySQL, 259
- host bus adapter icon, 244
- host group icon, 245
- host icon, 244
- HOST table, for MySQL, 259
- HOSTHBAS table, for MySQL, 260
- HOSTLUNS table, for MySQL, 261
- HP-UX
  - uninstalling from, 22
- hub icon, 244

## I

- icons
  - ASM switch, 244
  - blade switch, 244
  - bridge, 244
  - bridge group, 245
  - device, 243
  - director, 243, 244
  - enclosure group, 245
  - fabric group, 245
  - FCIP bridge, 244
  - FCIP bridge group, 245
  - FCIP gateway, 244
  - FCIP gateway group, 245
  - host, 244
  - host bus adapter, 244
  - host group, 245
  - hub, 244
  - iSCSI, 245
  - iSCSI bridge, 244
  - iSCSI bridge group, 245
  - iSCSI device, 244
  - iSCSI gateway, 244
  - iSCSI gateway group, 245
  - isolated group, 245

- JBOD, 244
- JDISK, 244
- loop, 244
- loop group, 245
- mSAN group, 245
- network attached storage, 244
- persisted fabric, 195
- persisted fabrics, 195
- products, 243
- routed in fabric group, 245
- routed in group, 245
- routed in router fabric group, 245
- SAN router, 243
- SAN Router group, 245
- server, 244
- storage, 244
- storage group, 245
- switch group, 245
- tape, 244
- tape group, 245
- unknown device, 244
- virtual device group, 245
- icons iSCSI device group, 245
- import feature, 285
- importing, 109, 116
- in-band discovery
  - overview, 132
- in-band discovery, enabling, 139
- information bar, 68
- installing
  - EFCM, 13
  - license key, 10
  - on UNIX systems, 16
  - on Windows systems, 13
- IP addresses
  - adding, 142
  - changing, 144
  - removing, 147
- iSCSI bridge group icon, 245
- iSCSI bridge icon, 244
- iSCSI device group icon, 245
- iSCSI device icon, 244
- iSCSI gateway group icon, 245
- iSCSI gateway icon, 244
- iSCSI icon, 245
- ISLs, clearing alerts, 196
- isolated group icon, 245

## J

- JBOD icon, 244
- JDISK icon, 244

## K

- keyboard shortcuts, 247

## L

- launching
  - applications, 129
  - Element Managers, 128
  - Telnet session, 127
- launching SAN Management application, 23
- layout, changing in persisted fabrics, 196
- license key
  - installing, 10
  - retrieving, 11
  - upgrading, 10
- license update feature, 285
- license, See license key
- life cycle of a SAN, 54
- Linux
  - uninstalling from, 22
- log entries, copying, 219
- log file, location, 58
- log management feature, 285
- logging in, 73
- logging out, 74
- logs
  - clearing, 217
  - exporting, 217
  - overview, 58, 216
  - viewing, 216, 218
- loop group icon, 245
- loop icon, 244
- LUN management feature, 285
- LUN table, for MySQL, 262

## M

- main window, 55
- managing reports, 223
- managing users, overview, 89
- map area, 55
- map editing feature, 285
- map HBA to server feature, 285
- map loop to hub feature, 285
- map port to storage feature, 285
- master log
  - copying from, 219
  - filtering, 218
  - icons, 246
  - illustrated, 58
  - location, 58
  - overview, 58
- menu bar
  - Edit, 60
  - Plan, 63
  - SAN, 60
  - View, 61
- menu bar, Configure, 64
- menu bar, Discover, 63
- menu bar, Help, 66
- menu bar, Monitor, 65
- menu bar, Tools, 66
- merging, persisted fabrics, 196
- minimap
  - attaching, 59
  - detaching, 59
  - overview, 59
  - resizing, 59
- minus icon, persisted fabrics, 195
- monitor ethernet event feature, 286
- Monitor menu, 65
- monitoring events, 216
- mSAN group icon, 245
- MySQL database, setting up, 115

## N

- network attached storage icon, 244
- new features, licensing, 10
- new features, ordering, 10
- notifications
  - configuring e-mail, 220
  - overview, 220

## O

- offline icon, 246
- online help, searching, 52
- opening
  - EFCM, 23
- operational icon, 246
- ordering upgrades, 10
- out-of-band discovery
  - overview, 132
  - setting up, 139

## P

- pasting events from logs, 219
- performance feature, 286
- persist fabric feature, 286
- persisted fabrics
  - clearing alerts, 196
  - connection status, determining, 196
  - determining status, 195
  - finding devices in, 197
  - icon, 195
  - icons, 195
  - layout changes, 196
  - merging, 196
  - minus icon, 195
  - plus icon, 195
  - principal switches in, 196
  - splitting, 196
- persisting fabrics, 194
- physical map
  - exporting, 109
  - printing, 226
  - zooming in, 103
  - zooming out, 103
- Plan menu, 63
- planning feature, 286
- plus icon, persisted fabrics, 195
- polling client, 250
  - configure for faster logins, 250
  - forcing all clients as polling, 251
- polling delay, setting, 141
- polling parameters, changing, 141
- port fencing feature, 286
- PORT table, for MySQL, 264
- principal switches, in persisted fabrics, 196

- printing
  - physical map, 226
  - topology, 226
- printing reports, 226
- privileges
  - user groups, 272
- product list
  - exporting, 109
  - overview, 56
  - viewing, 56
- product status icons, 246
- product status log
  - copying from, 219
  - overview, 216
- product status, determining, 164
- products
  - changing properties, 163
  - changing types, 163
  - determining problems, 164
  - determining status, 164
  - finding, 163
  - finding in persisted fabrics, 197
  - icons, 243
  - searching for, 163
  - status icons, 246
  - status, determining, 68
  - unpersisting, 194
- properties edit feature, 286
- properties, device route, 166

## R

- read/write permissions, assigning to views, 95
- REALTIMEPERFORMANCE table, for MySQL, 265
- release 2.7, upgrading from, 10
- remote access
  - configuring, 100
- remote access feature, 286
- removing
  - community strings, 213
  - device shortcut menu option, 127
  - IP addresses, 147
  - servers, 78
  - tools, 124
  - Tools menu options, 125
  - trap recipients, 198
  - users, 91
- removing trap recipients, 211
- removing user groups, 97

- removing users from groups, 99
- renaming servers, 78
- report feature, 286
- reports
  - deleting, 227
  - generating, 224
  - generating for routers, 227
  - generating for zone library, 228
  - overview, 223
  - printing, 226
  - viewing, 225
- requirements, system, 4
- retrieving license key, 11
- routed in fabric group icon, 245
- routed in group icon, 245
- routed in router fabric group icon, 245
- routers, blocked broadcast request, 230
- routes
  - hiding, 166
  - showing, 165
  - viewing, 166
- running
  - EFCM, 23

## S

- SAN files
  - exporting, 109
  - importing, 116
- SAN Management application
  - starting, 23
- SAN menu, 60
- SAN Router group icon, 245
- SAN router icon, 243
- searching
  - for products, 163
  - online help, 52
- security admin feature, 286
- server icon, 244
- server name, determining, 69
- servers
  - adding, 75, 78
  - associating to HBAs, 77
  - determining name, 69
  - logging in, 73
  - logging out, 74
  - removing, 78
  - renaming, 78
  - sessions, 101

- service, requesting, 164
- session log
  - copying from, 219
  - overview, 216
- sessions
  - specifying, 100
  - viewing, 101
- setting
  - discovery, 139
  - polling delay, 141
- setup tools feature, 286
- shortcut menu
  - adding option to, 126
  - changing, 127
  - removing option from, 127
- shortcuts, 247
- show route feature, 286
- show routes
  - overview, 165
  - procedure, 165
  - requirements, 165, 182
- showing levels of detail, physical map, 104
- shutdown feature, 286
- sniffer
  - events in log, 199
  - refreshing, 206
- sniffer session
  - deleting, 205
  - stopping, 203
- sniffer test
  - adding, 201
  - deleting, 205
  - editing, 204
  - running, 202
  - stopping, 203
  - viewing, 200
- snmp agent
  - configuring, 207
  - overview, 207
  - turning off, 208
  - turning on, 208
- SNMP agent configuration feature, 286
- SNMP trap events, changing TCP/IP ports, 214, 242
- software configuration properties feature, 286
- Solaris
  - uninstalling from, 22
- specifying remote access, 100
- splitting persisted fabrics, 196

- starting
  - EFCM, 23
  - Element Managers, 128
  - SAN Management application, 23
  - Telnet session, 127
- status bar, 68
- status, determining for fabric, 166
- storage group icon, 245
- storage icon, 244
- switch group icon, 245
- symapi.jar, class path issues, 232
- system requirements, 4

## T

- tape group icon, 245
- tape icon, 244
- TCP/IP ports, changing, 214, 242
- Telnet session, launching, 127
- terminating on UNIX, 16
- terminating on Windows, 13
- third-party applications, opening, 129
- time-out values, changing, 141
- tips, turning on and off, 104
- tool tips, turning on and off, 104
- toolbar, description, 67
- toolbox, description, 68
- tools
  - accessing, 123
  - adding, 123
  - adding to Tools menu, 124
  - changing on Tools menu, 125
  - opening from, 129
  - removing, 124
- Tools menu, 66
  - adding an option, 124
  - changing an option, 125
  - removing an option, 125
- topology, See physical map
- total user count, 69
- trap forwarding feature, 286
- trap forwarding, configuring, 197
- trap recipients
  - adding, 198, 209, 211
  - configuring, 207
  - editing, 210
  - overview, 207
  - removing, 198, 211

- troubleshooting
  - addresses, 229
  - discovery, 230
  - fabric binding, 233
  - import issue, 235
  - installation issue, 235
  - LUNs, 233
  - managing Cisco switches, 236
  - mapping loop to hub, 235
  - miscellaneous problems, 234
  - products, 234
  - server startup issue, 236
  - server-client communication issue, 235
  - Windows service issue, 236
- turning off discovery, 151
- turning on discovery, 151

## U

- unassociating, HBA to server, 77
- uninstalling
  - EFCM, 21
  - from AIX systems, 22
  - from HP-UX systems, 22
  - from Linux systems, 22
  - from Solaris systems, 22
  - from UNIX systems, 21
  - on Windows systems, 21
- UNIX
  - installing on, 16
  - uninstalling from, 21
- UNIX, terminating the application, 16
- unknown device icon, 244
- unknown icon, 246
- unpersisting fabrics, 194
- unpersisting products, 194
- upgrading
  - license key, 10
  - SAN Management application, 10
- user group
  - access levels, 285
  - privileges, 272
- user groups
  - creating, 94
  - editing, 96
  - removing, 97
- user ID, determining, 69
- user list, viewing, 89
- user management feature, 286

- user privileges
  - defined, 272
- users
  - access levels, 285
  - adding, 90
  - assigning to groups, 98
  - changing, 91
  - determining permissions, 99
  - filtering events for, 92
  - finding in groups, 99
  - groups, 285
  - managing, overview, 89
  - privileges, 272
  - removing, 91
  - removing from groups, 99
  - viewing all, 89
- users, total, 69

## V

- version 2.7, upgrading from, 10
- view management feature, 286
- View menu, 61
- view options, changing, 103
- viewing
  - active sessions, 101
  - events, 216
  - fabric events, 218
  - product list, 56
  - reports, 225
  - routes, 166
  - users, 89
  - zooming in, 103
  - zooming out, 103
- views, changing permissions, 96
- virtual device group icon, 245
- virtual fabric feature, 286

## W

- Windows
  - installing on, 13
  - terminating the application, 13
  - uninstalling from, 21

## Z

ZONE table, 267

ZONELIBRARY table, for MySQL, 268

ZONEMEMBER table, for MySQL, 268

ZONESET table, for MySQL, 270

ZONESETZONES table, for MySQL, 270

zooming in, 103

zooming out, 103